Tampereen yliopisto

Santeri Taskinen

KYBERTILANNEKESKUS

– resilientin nykyorganisaation hermokeskus

Johtamisen ja talouden tiedekunta
Pro gradu -tutkielma
Syyskuu 2019


KYBERTILANNEKESKUS
RESILIENTIN NYKYORGANISAATION HERMOKESKUS

TASKINEN Santeri Mikael
Kybertilannekeskus – resilientin nykyorganisaation hermokeskus
Pro gradu -tutkielma
Tampereen yliopisto, Hallintotieteiden tutkinto-ohjelma
Turvallisuushallinnon maisteriohjelma
Syyskuu 2019

TIIVISTELMÄ

Tässä tutkimuksessa selvitetään, *miten kybertilannekeskus vaikuttaa organisaation kyberresilienssiin*. **Kyberresilienssi** on organisaation kykyä jatkaa toimintaansa haitallisista kybertapahtumista huolimatta. **Kybertilannekeskus** (CSOC) on tukiorganisaatio, jossa asiakasorganisaation kyberavaruuden muutosvoimien tietoteknisellä havaitsemiskyvyllä aistittavien tilannetietojen merkityksiä tulkitaan tilannekuvaksi. Se yhdistetään ihmisten kokemuksen, kyvykkyyksien ja taitojen avulla tilanneymmärrykseksi. Tämän perusteella päätellään asiakasorganisaation kyberavaruuden muutosvoimien aiheuttamille uhille viisaita tilannevasteita eli ratkaisuja. Kybertilannekeskuksen tehtävänä on luoda tilannetietoisuutta, jolla kyberresilienssin määrää on mahdollista säätää oikealle tasolle. Tämä taso määritellään ja saavutetaan varautumisen avulla, jossa yhdistyvät jatkuvuus- ja palautumissuunnittelun menetelmät.

Tutkimuksen teoriatausta perustuu **järjestelmäteoriaan**, jonka mukaan organisaatiot ovat avoimia ympäristöstään riippuvaisia kokonaisvaltaisia järjestelmiä. Organisaatiot pyrkivät tavoitteidensa täyttämiseen itsesäätelyn, järjestäytymisen ja kasvun avulla. Kybertilannekeskuksen vaikutuksia mallinnetaan tässä tutkimuksessa kehitellyllä kuuden teoreettisen mallin yhdistelmällä, joka noudattelee järjestelmäteorian suuntauksen – kybernetiikan – periaatteita. Kybernetiikka on viestintä- ja hallintajärjestelmien tutkimiseen kehitelty teoreettinen suuntaus, jossa järjestelmät mukautuvat ympäristön muutoksiin saamansa palautteen pohjalta. Kybertilannekeskus toimii kyberneettisen mukautumisen mahdollistajana.

Tutkimuksen tieteenfilosofia perustuu interpretivistiseen tulkinnallisuutta korostavaan otteeseen. Tutkimusstrategia on hermeneuttinen, jossa tietoa tuotetaan hahmottamalla asioiden välisiä suhteita ja tulkintoja kehämäisesti. Aineistonhankintamenetelmänä on **kvalitatiivinen** puolistrukturoitu seitsemän kyberturvallisuusasiantuntijan **teemahaastattelu**, joka toteutettiin vuonna 2018 Cyber Security Nordic -messuilla Helsingin messukeskuksessa. Aineistona on lisäksi yli 200 muuta kirjallista lähdettä. Tutkimuksessa määritellään tarvittavat käsitteet, taustat ja aineiston analyysimenetelmät tutkimustuloksen validiteetin ja reliabiliteetin varmistamiseksi.

Tuloksien mukaan organisaation kyberresilienssiin vaikuttavat (1) teknisten ratkaisuiden, (2) prosessien, (3) ihmisten ja (4) johtamisen osa-alueet. Kybertilannekeskus vaikuttaa osa-alueisiin (1) tilannetietoisuus- ja (2) varautumistoimintojen avulla kyberresilienssiä parantavasti. Kybertilannekeskuksen **tilannetietoisuustoiminto** parantaa tilannetietojen keräämisen teknistä laajuutta ja hyödynnettävyyttä. Johtajien päätöksentekoedellytykset selkeytyvät ja nopeutuvat. Lisäksi resursseja käytetään tehokkaammin, ratkaisujen löytymisprosessi nopeutuu ja ihmisten koulutus sekä kokemus tukevat parempaa resilienssiä. **Varautumistoiminnolla** parannetaan jatkuvuus- ja toipumissuunnittelun mukaisia prosesseja yhteistyön ja harjoitusten avulla. Käytettävien tietojärjestelmien kestävyyteen ja nopeaan palautumiskykyyn sekä varajärjestelyihin kiinnitetään enemmän huomiota. Henkilökuntaa koulutetaan ja varataan riittävästi häiriötilanteita varten. Lisäksi resurssien suunnittelu on pitkäjänteisempää.

Nykyorganisaatiot ovat digitalisaation myötä jatkuvasti riippuvaisempia kyberavaruuden mahdollisuuksista ja uhista. Tutkimustuloksen perusteella organisaatioiden tulisi kyetä tiedostamaan ja varautumaan paremmin muuttuviin kyberuhkiin. Kybertilannekeskus on kyberavaruuden **hermokeskuksena** yksi työkalu parempaa kyberresilienssiä tavoittelevalle nykyorganisaatiolle.

Avainsanat: kybertilannekeskus, kyberresilienssi, kyberturvallisuus, kybertilannekuva, kybertilannetietoisuus, varautumissuunnittelu, järjestelmäteoria ja kybernetiikka.

Tämän julkaisun alkuperäisyys on tarkastettu *TurnitIn OriginalityCheck* –ohjelmalla.

TASKINEN Santeri Mikael
Cybersecurity Operations Center – Nerves of Modern and Resilient Organization
Master's thesis
Tampere University, Master of Administrative Science degree program
Master's Programme in Security Management
September 2019

ABSTRACT

This study explores *how Cybersecurity Operations Center affects to cyber resilience of an organization*. **Cyber resilience** is ability of an organization to continue to operate despite malicious cyber events. **Cybersecurity Operations Center** (CSOC) is a supportive organization which interprets the meaning of situational data, as perceived by the client organizations computational capability of cyberspace changes. It combines people's experience, abilities and skills into situational knowledge. Based on this, wise situational responses, or solutions, are drawn against the threats posed by changes of cyberspace. The mission of the CSOC is to create situational awareness that allows client organization to adjust the amount of cyber resilience to the appropriate level. This level is defined and achieved through preparedness, which combines continuity and recovery planning methods.

The theoretical background of the study is based on **systems theory**, which states that organizations are open systems that are dependent on their environment and that seek to achieve their goals through self-regulation, organization and growth. The effects of the CSOC are modeled using a developed combination of six theoretical models that follow the principles of systems theory orientation called cybernetics. Cybernetics is a theoretical orientation developed for the study of communication and control systems, in which systems adapt to the changes they receive in response to changes in the environment. In this matter Cybersecurity Operations Center acts as a cybernetic resilience facilitator.

The research philosophy is based on an interpretivist approach that emphasizes interpretability. The research strategy is hermeneutic, in which knowledge is produced by circumscribing relationships and interpretations. The material acquisition method is a **qualitative semi-structured interview** with seven cyber security experts, which was conducted in 2018 at the Cyber Security Nordic exposition in Helsinki. In addition, there are over 200 other written sources used. The study defines the necessary concepts, backgrounds and data analysis methods to ensure validity and reliability of the research result.

According to the results, the cyber resilience of an organization is affected by (1) technical solutions, (2) processes, (3) people and (4) leadership. (1) Situational awareness and (2) emergency response functions are enhanced by the CSOC to improve cyber resilience. CSOC 's **situational awareness function** improves the technical scope and usability of collecting situational data. The decision-making conditions for managers are clarified and accelerated. In addition, resources are used more efficiently, the process of finding solutions is faster, and people's knowledge and experience support resilience better. **Preparedness function** improves continuity and recovery planning processes through collaboration and exercises. More attention is being paid to the durability and rapid recovery of the information systems used and back-up arrangements adequacy. Personnel are adequately trained and equipped to deal with disruptions. In addition, resource planning is more far fetching.

As a result of digitalization, today's organizations are increasingly dependent on the opportunities and threats of cyberspace. Based on the research findings in this study, organizations should be able to be more aware and prepared for changing cyber threats. Acting as **a nerve center** for cyberspace, the Cybersecurity Operations Center is one tool for today's organization seeking for better cyber resilience.

Keywords: Cybersecurity Operations Center (CSOC), Cyberresilience, Cybersecurity, Cyber situational picture, Cyber situational awareness, Contingency planning, Systems Theory and Cybernetics.

This publication originality is verified with *TurnitIn OriginalityCheck* -program

SISÄLLYS

TAULUKKOLUETTELO

KUVIOLUETTELO

KUVALUETTELO

LYHENNELUETTELO

APT	**Advanced Persistent Threat**, kyvykäs, pysyvä ja kohdistettu uhka
BCP	**Business Continuity Planning**, jatkuvuussuunnittelu
BIA	**Business Impact Analysis**, toimintojen vaikutusanalyysi
BKT	**Bruttokansantuote**
CSIS	**Center for Strategic and International Studies**, CSIS-tutkimuslaitos
CSOC	**Cyber Security Operations Center**, kybertilannekeskus
DIKW	**Data, Information, Knowledge ja Wisdom**, Data, Informaation, Tietämys ja Viisaus
DRP	**Disaster Recovery Planning**, toipumissuunnittelu
FAAMG	**Facebook, Apple, Amazon, Google ja Microsoft**, FAAMG-yhtiöt
GDPR	**General Data Protection Regulation**, EU:n yleinen tietosuoja-asetus
GST	**General System Theory**, yleinen järjestelmäteoria
IBCDRP	**Integrated Business Continuity and Disaster Recovery Planning**, yhdistetty jatkuvuus- ja toipumissuunnittelun malli
ICANN	**Internet Corporation for Assigned Names and Numbers**, ICANN-yhtiö
IDS	**Intrusion Detection System**, tunkeutumisen havaitsemisjärjestelmä
IoT	**Internet of Things**, esineiden internet
IP	**Internet Protocol**, verkkokerroksen protokolla
IPS	**Intrusion Prevention System**, tunkeutumisen estojärjestelmä
IRC	**Internet Relay Chat**, internetin pikaviestipalvelu
ISAC	**Information Sharing and Analysis Center**, yhteistyöverkosto
ISO/IEC	**International Organization for Standardization**, kansainvälinen standardoimisorganisaatio
MBCO	**Minimum Business Continuity Objective**, alin siedettävä toimintotaso
MTPD	**Maximum Tolerable Period of Disruption**, pisin siedettävä häiriöaika
NIS	**Directive on Security of Network and Information Systems**, verkko- ja tietoturvadirektiivi
OSINT	**Open Source Intelligence**, avointen lähteiden tiedustelu
RPO	**Recovery Point Objective**, palautumistaso
RTO	**Recovery Time Objective**, mukautumisaika
SIEM	**Security Incident and Event Management**, turvallisuustapahtumien hallintajärjestelmä
SLA	**Service Level Agreement**, palvelutasosopimus
SOC	**Security Operations Center**, turvallisuusoperaatiokeskus tai kybertilannekeskus
SWIFT	**Society for Worldwide Interbank Financial Telecommunication**, SWIFT-yhteisö
TEMPEST	**Transient Electromagnetic Pulse Emanation Standard**, säteilyturvallisuus
UEM	**Unified Endpoint Management**, päätelaitehallinta
VLSI	**Very Large Scale Integration**, erittäin suurikokoiset pii-puolijohdemikrosirut
VPN	**Virtual Private Network**, virtuaalinen erillisverkko

1 JOHDANTO

”Vain muutos on pysyvää” oli antiikin filosofin Herakleitoksen lentävä lausahdus. Nykyisessä globaalissa, verkottuneessa ja teknologiavaltaisessa yhteiskunnassa muutoskaan ei ole luonteeltaan pysyvää, tasaista ja aina samanlaista. Päinvastoin nykytilanteen hahmottaminen – puhumattakaan tulevaisuuden ennustamisesta – tuntuu haastavalta, mutkikkaalta ja monisyiseltä. Mistä vaikea nykytilanteen selvittäminen johtuu? Millaisia ominaisuuksia organisaatioilta vaaditaan nykyisistä tietoteknisistä haasteista selviytymiseen? Miten nykytilanteesta tietoisena oleminen ja varautuminen vaikuttavat organisaatioiden kykyyn mukautua muuttuviin olosuhteisiin?

Nykypäivän tavoitteellisten organisaatioiden toimintaympäristö on moniulotteinen. Organisaatioiden fyysisen maailman haasteet, kuten maantieteellinen sijainti, aikariippuvaisuus ja toimintojen tehokkuus ovat jatkuvasti kehitettäviä osa-alueita. Kaikkiin näihin haasteisiin on voitu vaikuttaa digitalisaation, verkostoitumisen ja tietoteknisten ratkaisujen avulla. Teknologinen muutos on ollut monien organisaatioiden avain menestykseen. Esimerkiksi yksityiset niin sanotut FAAMG-yhtiöt eli Facebook, Apple, Amazon, Google (Alphabet) ja Microsoft ovat markkina-arvoltaan maailman suurimpia yhtiöitä ja kaikki teknologiayhtiöitä eli täysin riippuvaisia ja samalla vastuussa kyberavaruuden toimivuudesta (Goldman Sachs 2017, 1).

Kansallisvaltioittain tarkasteluna Yhdysvallat, Kiina, Korea, Japani, Saksa, Ranska, Ruotsi ja Kanada yltävät korkeimmille sijoille vertailtaessa 25 nopeimmin kehittyvää teknologian osa-aluetta patenttimäärillä vuosina 2013-2016 (OECD 2019, 30). Vertailtaessa kaikkien maailman maiden bruttokansantuotteita huomataan, että edellä luetellut digiajan edelläkävijävaltiot löytyvät korkeilta sijoilta myös BKT-tilastoista (The World Bank 2019). Teknologinen muutos on tuonut organisaatioille vaurautta, toimeentuloa ja tehokkuutta. Samalla organisaatioista on tullut alttiita kyberavaruuden haitallisille vaikutuksille.

Riippumaton Center for Strategic and International Studies (CSIS) -tutkimuslaitos on listannut maailmanlaajuisesti keskeisiä kyberpoikkeamia, jotka ovat kohdistuneet valtioiden virastoihin, puolustus- ja korkean teknologian yrityksiin tai aiheuttaneet yli miljoonan dollarin taloudelliset menetykset. Listauksessa on 13 vuoden ajalta yli 440 kyberpoikkeamaa

vuosien 2006 toukokuusta 2019 toukokuuhun. Listauksesta puuttuvat salatut tapaukset ja alle miljoonan dollarin menetykset aiheuttanut kyberrikollisuus. Osa tapauksista on jäänyt tiedostamatta huonon kyberavaruuden havainnointikyvykkyyden johdosta. (CSIS 2019) Viimeisen kymmenen vuoden aikana kyberpoikkeamien määrä on noussut ja/tai kyberpoikkeamien havainnointi- ja raportointikyky on parantunut. Seuraavat 11 konkreettista esimerkkiä kyberpoikkeamista perustelevat kyberhavainnointikyvyn ja siihen liittyvien vaatimusten täyttymisen tärkeyttä, tilanteen kehitystä ja tutkimusaiheen ajankohtaisuutta.

Listan ensimmäinen tapahtuma on vuodelta **2006**, jolloin Yhdysvaltain ulkoministeriön tietoverkkoihin tunkeuduttiin ja erilaisia tietoja ladattiin teratavujen verran ulkomaisten tahojen toimesta. Tapauksesta annettu sitaatti selittää hyvin, mikä useissa kyberpoikkeamissa toistuu vuodesta toiseen: "*Mikäli Kiinalaiset tai Venäläiset vakoojat olisivat peruuttaneet rekalla ulkoministeriön rakennukselle, rikkoneet lasiovet, sitoneet vartijat ja viettäneet yön kärräämällä mappeja rekkaan, olisi se voitu nähdä sodan julistuksena. Kun se tapahtuu kyberavaruudessa, tuskin edes huomaamme sitä.*" (CSIS 2019, 37)

Vuosi **2007** tunnetaan Viron ja Venäjän välisestä pronssisoturikiistasta, jossa neuvostoaikaisen miehityksen patsas haluttiin siirtää syrjäisempään paikkaan. Tapaus johti mellakoihin maan sisällä. Tapahtumiin vaikutettiin myös maan ulkopuolelta kyberavaruuden kautta. Viro oli jo vuonna 2007 hyvin tietoteknisesti verkottunut maa ja kyberhyökkäyksille altis. Hajautettu palvelunestohyökkäys (engl. Distributed Denial of Service) lamautti Virossa verkkopankkipalveluita, medioiden uutissivustoja ja valtion sähköisiä palveluita. Myöhemmin hyökkäykset laajenivat puhelinverkkoja, maksuliikennejärjestelmiä ja Internetin keskeisiä osia koskeviksi. Tapausta on pidetty yhtenä varhaisista kybersodankäynnin operaatioista. Hyökkäysten tekijöitä ei ole saatu selville, tosin Venäjä ei antanut apua hyökkäysten torjumiseksi verkkojensa kautta. Parempi kybertoiminnan havainnointikyky olisi voinut auttaa Viroa yhteiskunnan palveluiden jatkuvuuden turvaamisessa. Tapauksesta seurasi hyvääkin: Viron kyberresilienssin paranemista, sillä Tallinnaan perustettiin vuonna 2008 Naton yhteistoiminnallisen kyberpuolustuksen huippuyksikkö (NATO CCD COE) parantamaan kyberpuolustuksen tasoa. Samalla Virossa on opittu tapahtuneesta, nostettu hyökkääjien kynnystä toimia kiinni jäämättä ja varauduttu tuleviin uhkiin entistä resilientimmin. (Clarke & Knake 2010, 13-15; CSIS 2019, 37; Herzog 2011, 56)

Vuonna **2009** tuli julkisuuteen valtiollisen toimijan tekemä kyberase ”STUXNET”, jonka tavoitteena oli iranilaisten voimalaitosten ja/tai kaasuputkien loogisten ohjausyksikköjen uudelleenohjelmointi toimimaan virheellisesti. Ase toimi tavoitteensa mukaisesti ja levisi muistitikulla internetistä eristettyyn ydinlaitokseen hidastaen Iranin ydinohjelmaa. (Chen & Abu-Nimeh 2011, 92; CSIS 2019, 31; Falliere, Murchu & Chien 2011, 2-4 ja 29-30)

Esimerkki osoittaa kybersodankäynnin mahdollisuuden, tehokkuuden ja todellisuuden. Tapauksen myötä on yleisesti hyväksytty, että kaikilta uhilta on käytännössä mahdoton puolustautua – hyvistä turvajärjestelmistä huolimatta kyberpoikkeamia tapahtuu. Hyvässä tapauksessa poikkeama huomataan ja palautuminen aloitetaan nopeasti. Huonossa tapauksessa kaikki jää huomaamatta ja lisätuhot ovat mahdollisia.

Vuonna **2010** yhdysvaltalaisen Nasdaq-arvopaperipörssin internet-sovellus ”Directors Desk” joutui kybervakoilun kohteeksi. Directors Deskillä eri yhtiöiden hallitukset jakoivat luottamuksellisia dokumentteja ja kommunikoivat toimitusjohtajiensa kanssa. Nasdaqin vakoilijoilla oli pääsy näihin tietoihin, eikä selvyyttä ole saatu siitä, kuinka kauan tiedot ovat altistuneet vakoilulle. (CSIS 2019, 31; Finkle 2011)

Edellinen tapaus osoittaa kaikista kybertapahtumista tallennettavien kirjausten eli lokitusten tärkeyden. Ilman lokitusta ongelmia ei voida selvittää ja kybertilannekuvan muodostaminen on käytännössä mahdotonta.

Vuonna **2013** MTV3 Uutiset raportoi kevättalvella havaitusta jopa neljä vuotta kestäneestä Suomen ulkoministeriöön kohdistuneesta verkkovakoilusta. Vuonna 2016 hyökkääjäksi selvisi ”Uroburos”-haittaohjelman vakoilujälkien häivytykseen käytetyn satelliittilinkkipohjaisen menetelmän perusteella venäläinen verkkovakoojaryhmä ”Turla”, jota rahoittaa Venäjän valtio (Kerkkänen & Pietarinen 2016). Ulkoministeriö ei itse havainnut tapahtunutta, vaan sai asiasta vinkin ulkomaiselta taholta Suojelupoliisin ja silloisen Viestintäviraston CERT.fi:n eli kansallisen tietoturvaviranomaisen kautta. (CSIS 2019, 24; Haapala 2013) Mikäli tapaus oltaisiin havaittu aikaisemmin paremman kybertilannekuvan avulla, oltaisiin voitu vastatoimiin ryhtyä jo paljon aikaisemmin ja diplomaattinen arvovaltatappio sekä tietojen menetys estää tai sen vaikutuksia vähentää.

Marraskuussa **2014** Pohjois-Koreasta lähtöisin ollut tietomurto ja terroriuhkaus elokuvayhtiö Sony Picturesille johti Pohjois-Korean johtajan salamurhasta kertovat elokuvan teatteri-

julkaisujen perumiseen. (CSIS 2019, 23; Hallamaa 2014) Tapaus todistaa, että kyberhyökkäyksillä voidaan kiristää, painostaa, näyttää kyvykkyyttä ja saada aikaan pelotevaikutusta haluttujen tulosten saavuttamiseksi mitä erilaisemmissa kohteissa.

Tammikuussa **2015** hakkerit käyttivät sosiaalista manipulointia ja pääsivät käsiksi saksalaisen terästeollisuuslaitoksen automaatiojärjestelmään. Hyökkääjät aiheuttivat tehtaan tulipesän sammumattomuuden, joka aiheutti valtavat fyysiset tuhot tehtaalla. (CSIS 2019, 23; Lee, Assante & Conway 2014, 1 ja 7) Esimerkki todistaa kyberavaruuden turvallisuuden suoran yhteyden ja vaikutukset fyysisen maailman turvallisuuteen.

Helmikuussa **2016** tapahtui yksi historian suurimmista kybervarkauksista, kun hakkerit onnistuivat siirtämään 81 miljoonaa dollaria Bangladeshin keskuspankin tililtä New Yorkin keskuspankista valeidentiteeteillä perustetuille filippiiniläisille tileille. Hyökkäys onnistui lähettämällä 35 tekaistua siirtomääräystä – miljardin dollarin arvosta– Bangladeshin keskuspankin kautta kansainvälisellä SWIFT-järjestelmällä, jota käytetään rahansiirtotietojen välittämiseen pankkien välillä. New Yorkin keskuspankki hyväksyi neljä näistä määräyksistä, vaikka ne olivat poikkeuksellisia: väärin muotoiltu, osoitettu yksityishenkilöille ja tavallisesta Bangladeshin keskuspankin toiminnasta poikkeavia. Lähes 63 miljoonaa dollaria on edelleen kateissa, eikä anomalioita eli normaalista poikkeavia toimintoja havaittu ajoissa. Tämä johtui siitä, että New Yorkin keskuspankilta puuttui reaaliaikainen järjestelmä kyberpoikkeamien havaitsemiseen. Maksut tarkastettiin vasta jälkikäteen manuaalisesti. Tapaus osoittaa reaaliaikaisuuden ja poikkeamien havaitsemisen tärkeyden nykyisessä aikakriittisessä kyberavaruudessa toimittaessa. (CSIS 2019, 19-20; Das & Spicer 2016)

Kesäkuussa **2017** tiedot salaava kiristyshaittaohjelma nimeltään ”NotPetya” pysäytti Kööpenhaminassa pääkonttoriaan pitävän maailman suurimman laivausyhtiön Møller-Maerskin satamat kahdeksi päiväksi, kun yhtiön tietokoneet saastuivat ja koko tietoverkko oli rakennettava uudelleen. Yhtiö joutui digiaikana turvautumaan manuaaliseen operointiin ja yhtiön toiminnan jatkuvuuden turvaamiseen, laivojen lipuessa satamiin 15 minuutin välein. Poikkeama aiheutti ainakin 300 miljoonan dollarin kustannukset. Yhtiö selvisi tilanteesta ja palautui työntekijöiden ansiosta hyvin laajan ja ajantasaisen avoimen tilannekuvan jakamisen sekä asiantuntijayhteistyöverkostonsa avulla rakentaen koko tieto- ja viestintäteknologiainfrastruktuurinsa uudelleen vain noin 10 päivässä. (CSIS 2019, 15; Palmer 2019)

Vuoden **2018** heinäkuussa järjestettiin Helsingissä presidenttien Trump ja Putin välinen huippukokous. Se aiheutti 2-4 päivää ennen kokousta etenkin Kiinasta – 29 prosenttia kokonaismäärästä – havaitun esineiden internetin (IoT) laitteisiin kohdistuneen, niin sanotun ”brute force” eli salasanan arvaamiseen perustuvien hyökkäysyritysten määrän rajun nousun. Hyökkäysten kohteena olivat erityisesti laitteet, jotka välittävät kuvaa tai ääntä, kuten konferenssipuhelimet. Venäjän alueelta tulevien hyökkäyksien osuus väheni normaalista 14 prosentista 7 prosenttiin, mutta USA:sta tulevat hyökkäykset pysyivät normaalilla tasolla noin 12-14 prosentissa kokonaismäärästä. Onnistuneiden hyökkäysten määrästä ei ole saatavilla tietoja. Tutkimuksen teki kansainvälinen F5 teknologiayhtiö, joka havainnoi ja valvoo jatkuvasti maailmalla isoja hyökkäysverkkoja eri maissa, kuten Kiinassa, Ranskassa ja Venäjällä. Nämä verkot tuottavat tyypillisesti suurimman osan hyökkäyksistä maailmalla. (Boddy & Shattuck 2018; CSIS 2019, 8)

Kybertilannekuvaa seurataankin maailmalla entistä tarkemmin ja etenkin tiedusteluelimet käyttävät kyberavaruuden mahdollisuuksia hyväksi.

Vuonna **2019** Suomessa eduskuntavaalien aikaan Keskusrikospoliisi tutki Oikeusrekisterikeskuksen vaalit.fi -tulospalveluun tehtyä lyhytkestoista ja heikohkoa palvelunestohyökkäystä. Tämän tutkimuksen kannalta tapauksesta tekee mielenkiintoisen se, että valtion tieto- ja viestintätekniikkakeskus Valtorissa poikkeama huomattiin normaalin valvonnan yhteydessä, vaikka hyökkäys tehtiin aamuyön tunteina. Tapauksen johdosta ei nähty tarvetta havainnointikyvykkyyden lisäämiselle ja tapaukseen oli valmistauduttu etukäteen. Tilannekuvan seurannasta ja etukäteisvarautumisesta olikin hyötyä, eikä suuria haittoja palvelun käyttäjille koitunut. (CSIS 2019, 1; Konttinen 2019)

Muutos organisaatioiden toimintaympäristössä on ollut nopeaa. Osalle organisaatioista tietotekninen ja verkottunut kyberavaruus on ainoa mahdollisuus toimia järkevästi – toteuttaa ydintehtävät tehokkaasti. Lähes kaikki organisaatiot ovat kyberavaruuden vaikutusten kohteena tavalla tai toisella. Tämän tutkimuksen tematiikka onkin hyvin ajankohtainen. Edellä esitetyt viimeaikaiset tapaukset todistavat kybertilannekuvan ja tilanteenmukaisen toiminnan tärkeyden nykyorganisaatioissa, joiden edellytykset toimia ja täyttää tehtävänsä onnistuneesti riippuvat sähköisten järjestelmien jatkuvasta toiminnasta sekä organisaation kyvystä sietää muutoksia toimintaympäristössään. Organisaation ominaisuutta joustaa,

mukautua ja ennakoida muutoksia jatkuvan toiminnan varmistamiseksi kutsutaan resilienssiksi eli sopeutumiskyvyksi, vastustuskyvyksi tai suomalaisittain sisuksi.

Tässä tutkimusraportissa perehdytään erityisesti siihen, millainen merkitys ja vaikutus kybertilannetietoisuudella on verkottuneiden organisaatioiden kyberresilienssiin eli kykyyn jatkaa toimintaansa haitallisista kybertapahtumista huolimatta. Tämä on tärkeää tietää, sillä nykyinen fyysisen maailman turvallisuuteen kytkeytynyt kyberavaruus on täynnä uhkia, joista tietämättömyys johtaa huonoihin päätöksiin, ikäviin seurauksiin, ikävimmissä tapauksissa suuriin taloudellisiin menetyksiin tai jopa ihmisten kuolemaan.

Eräs mahdollinen ratkaisu kybertilannetietoisuuden parantamiseksi on kybertilannekeskus, joka on eräänlainen nykyorganisaation hermokeskus, aistikeskus tai näkökyky kyberavaruuteen. Miten kyberavaruuteen ylettyvä ”hermosto” erilaisine anturiaisteineen vaikuttaa nykyorganisaatioiden kyberresilienssiin? Siihenkin tämä tutkimusraportti pyrkii vastaamaan.

2 TUTKIMUKSEN MENETELMÄVALINNAT

2.1 Tutkimuskysymys ja tavoitteet

Turvallisuus on aina toiminut motiivina ihmisten väliselle yhteistoiminnalle ja organisoitumiselle. Jo muinaiset ihmiset perustivat yhteisöjä ja organisoituivat toistensa turvaksi, koska se nähtiin hyödylliseksi elämän jatkuvuuden kannalta. (Virta 2012, 118) Vastaavanlainen periaate toimii edelleen. Ihmisistä koostuvat organisaatiot luovat ja ylläpitävät turvallisuutta, järjestystä ja rauhaa. Turvallisuutta ylläpitäviä organisaatioita tutkitaan turvallisuushallinnon tieteenalalla, jonka piiriin tämä tutkimus kuuluu tietojenkäsittelytieteellisellä vivahteella. Tämä tutkimus onkin luonteeltaan monitieteinen.

Tässä tutkimuksessa ratkaistava tutkimusongelma liittyy kybertilannekeskusorganisaatioiden toimintaan ja vaikutuksiin osana organisaation kyberturvallisuuden kokonaisuutta. Tutkimusongelman asettelun motiivit ovat aihealueesta tehdyn tutkimuksen vähäisyys, ajankohtainen tematiikka ja tutkijan oma mielenkiinto aihetta kohtaan. Tutkimusongelmasta muodostettu **tutkimuskysymys** on ohjannut tutkimuksen tekemistä:

Miten kybertilannekeskus vaikuttaa organisaation kyberresilienssiin?

Tutkimuskysymys koostuu viidestä sanasta ja kahdesta semanttisesta kokonaisuudesta, joiden ymmärtäminen vaatii perusteluja. Sanojen tarkemmat määrittelyt esitetään luvussa 3.2.

Tutkimuskysymyksen kaksi sisällöllistä osaa ovat

1. kybertilannekeskuksen toiminta, olemus ja määritelmä sekä
2. yleisesti organisaatioiden kyberresilienssiin vaikuttavat tekijät.

Tutkimuskysymyksen asettelu sisältää kaksi organisaatiota, jotka ovat

1. kybertilannekeskus ja
2. sen asiakasorganisaatio (tutkimuskysymyksessä ”organisaatio”).

Yksinkertaistaen: tutkimuksessa pyritään selvittämään, miten organisaation yksi (1) toiminta vaikuttaa organisaation kaksi (2) ominaisuuteen nimeltä kyberresilienssi. Tutkimuk-

sen toteuttamiseksi on välttämätöntä tarkastella kybertilannekeskuksen (1) toimintaa empiirisenä ja teoreettisena ilmiönä. Lisäksi tutkimuskysymyksen ratkaisemiseksi on selvitettävä, millaiset tekijät vaikuttavat organisaatioiden (2) kyberresilienssiin?

Tutkimuskysymys on muodostettu sana kerrallaan siten, että jokaisella sanalla on tutkimusprosessia ohjaava merkitys. **Miten**-kysymyssana viittaa laadullisessa tutkimuksessa tutkimusongelmaan, jonka tavoitteena on ilmiön kuvaaminen ja ymmärtäminen (Saaranen-Kauppinen & Puusniekka 2006, tutkimusongelmat). Tässä tutkimuksessa tämä ilmiö eli kokemuksen kautta paljastuva empiirinen kokonaisuus on kybertilannekeskustoiminta (Tieteen termipankki 2019m). Samasta syystä toiseksi sanaksi on valittu **kybertilannekeskus**. Kolmantena sanana on verbi **vaikuttaa**, joka viittaa kybertilannekeskuksen toiminnan aiheuttaman muutoksen kohdistumiseen toisen organisaation ominaisuuteen nimeltä kyberresilienssi (MOT Sanakirjat 2019). Sanalla ei kuitenkaan tässä yhteydessä oteta kantaa vaikutuksen olemassaoloon – vaikutuksia ei välttämättä ole. ”Vaikuttaa”-verbin kanssa tässä tutkimuksessa käytetään myös sanaa ”vaikutus”, joka tarkoittaa syvälle ulottuvaa kohdistumista ja muutosta kohteessa tai hyötyjen ja haittojen punnintaa (Kotimaisten kielten keskus 2019). Neljäs ja viides sana ”**organisaatio**” ja ”**kyberresilienssi**” käsitellään yhdessä, sillä ne määrittelevät tutkimuksen kohteen ja kohteen ominaisuuden, joista tässä tutkimuksessa ollaan ensisijaisesti kiinnostuneita.

Tämän tutkimuksen tavoitteena on tarkastella kybertilannekeskusten toimintaa, vuorovaikutussuhteita ja tarkoitusta kyberturvallisuuskontekstissa sekä selvittää tekijöitä, jotka vaikuttavat yleisesti kaikkien organisaatioiden kyberresilienssiin tutkijan tekemien tulkintojen avulla. Tavoitteena on kyetä kuvaamaan organisaation kyberresilienssiin vaikuttavia tekijöitä useita koeteltuja teorioita yhdistelemällä. Tästä syystä tämän tutkimuksen tutkimusstrategia on hermeneuttinen, jossa tavoitellaan tutkimuskohteen syvällistä inhimillistä ymmärtämistä. (Lähdesmäki, Hurme, Koskimaa, Mikkola & Himberg 2015, hermeneuttinen tutkimus)

Lisäksi tutkimuksen tavoitteena on tuottaa uutta tietoa kyberturvallisuuden tilannetietoisuuteen ja tilannekuvaan liittyvistä tarpeista, haasteista ja mahdollisuuksista. Tavoitteeseen pääsemiseksi on ollut välttämätöntä perehtyä ja analysoida jo alalla tehtyä tutkimuskirjallisuutta, määritellä uusien käsitteiden suhteita, merkityksiä ja määrittelyitä sekä tuottaa täy-

sin uutta tutkimusmateriaalia. Kirjallisen tutkimusraportin tavoitteena on tuoda esille tutkimuksen kulku, periaatteet ja tulokset mahdollisimman lukijaystävällisesti, toistettavasti ja havainnollisesti. Tästä syystä raportissa esitetään myös monia tekstisisältöä selkiyttäviä kuvioita. Myös selkeään ilmaisutapaan on kiinnitetty erityistä huomiota.

2.2 Perustelut aihealueen rajauksille

Aihealueen laajuuden ja moniulotteisuuden takia on ollut välttämätöntä tehdä monia rajauksia, jotta opinnäytetyölle asetetut laajuus-, aihealue- ja muut vaatimukset täyttyvät. Jokainen aihealueen rajaus on kuitenkin perusteltu. Tässä tutkimuksessa käsitellään tilannekeskustoimintaa vain kyberturvallisuuden näkökulmasta, vaikka monia tämän tutkimuksen teoreettisia lähestymistapoja voidaan soveltaa millaiseen tahansa tilannekeskustoimintaan. Tässä tutkimuksessa ei käsitellä moniulotteista kyberturvallisuutta koko laajuudessaan, vaan näkökulma painottuu tilannetietoisuuden ja tilannekuvan luomisen kontekstiin.

Kyberturvallisuusalan tutkimusta on ollut moniulotteisesti ja runsaasti olemassa jo pitkään, joten tässä tutkimusraportissa ei ole mahdollisuutta kaiken kirjallisuuden tiivistämiseen tai läpikäyntiin. Kybertilannekeskuksen toimintaa, rakennetta ja tehtäviä käsitellään resilienssin ja tilannetietoisuuden näkökulmasta vain tarpeellisin osin tutkimuskysymyslähtöisesti. Lisäksi tässä tutkimusraportissa ei ole mahdollisuutta tai järkevää kuvata kybertilannekeskuksen toimintaa laajasti, sillä toiminnan, rakenteiden ja tehtävien kuvauksia löytyy jo varsin hyvin alan julkaisuista ja kirjoista.

Jokainen tutkimusraportti on aikansa tuote, mutta tässä tutkimuksessa on pyritty löytämään sellaisia kybertilannekuvaan ja kyberresilienssiin liittyviä ominaisuuksia, jotka liittyvät organisaatioihin, järjestelmiin ja systeemeihin yleensä – ei vain nykyhetken teknologisiin järjestelmiin – kuten tarkkoihin analyysityön teknisiin työkaluihin tai toimintatapoihin.

Tutkimuksen tavoitteena ei ole tehdä laajoja yksityiskohtaisia kuvauksia tekniikasta, joilla varsinaista kyberturvallisuustyötä käytännössä tehdään. Tämä johtuu tutkimuksen yhteiskuntatieteellis-, organisaatio- ja hallinnollispainotteisesta lähestymistavasta kyberturvallisuuteen. Tutkimuksen teknispainotteisen aiheen konkretisoitumisen vuoksi on kuitenkin välttämätöntä kertoa joitakin käytännön perusteita sekä esimerkkejä teknistä osaamista vaa-

tivista tilanteista. Näin ollen, tässä tutkimusraportissa ei lähtökohtaisesti käsitellä yksityiskohtiin meneviä käytännössä toteutettavia teknisiä kyberturvallisuusmenetelmiä, vaan esimerkkejä ja selvennyksiä esitetään vain tarpeellisin osin.

2.3 Tieteenfilosofiset valinnat ja metodologia

Jokaisella tutkimuksella on tekijänsä ja tekijällä on omat piilevät oletuksensa eli taustasitoumuksensa – filosofiset perusoletukset – maailmasta, ihmisistä ja tutkimuksesta ylipäätään. Näitä oletuksia ei arkisesti ajatella, mutta tutkimustyössä niiden tunnistaminen ja tietoinen valinta on tärkeää. Tieteenfilosofisilla valinnoilla määritellään tieteellisen tiedon luonne, pätevyys, hankintatavat, luokittelu ja tiedon lisääntyminen (Tieteen termipankki 2019n). Tässä empiirisessä tutkimuksessa tieteenfilosofiset valinnat perustuvat tieteenfilosofian taustalla vaikuttaviin neljään osa-alueeseen: ontologiaan, epistemologiaan, logiikkaan ja teleologiaan. (Hirsjärvi, Remes & Sajavaara 1997, 123-126) Ontologia ja epistemologia käsitellään tässä alaluvussa, logiikka käsitellään seuraavassa alaluvussa 2.4 ja teleologia eli tutkimuksen tavoite ja tarkoitus käsiteltiin jo aiemmin luvussa 2.1.

Ontologiassa tutkitaan todellisuuden luonnetta, kuten tutkimuskohteen ja sen ympäristön suhteiden syvällistä käsittämistä (Hirsjärvi ym. 1997, 124-125). Tämän tutkimuksen todellisuuskäsitys pohjautuu monismiin, jossa kaikkien olemassa olevien asioiden ajatellaan olevan palautettavissa yhteen alkutekijään (Tieteen termipankki 2019k). Tällä tieteenfilosofisella valinnalla otetaan etäisyyttä dualismiin ja pluralismiin, joissa kaiken olemassa olevan todellisuuden alkutekijänä nähdään olevan enemmän kuin yksi alkutekijä. Päinvastoin – kuten kartesiolaisessa dualismissa alkutekijöinä erotellaan henkiset ja aineelliset substanssit – tässä tutkimuksessa kaiken ajatellaan olevan lähtöisin aineesta (Tieteen termipankki 2019e). Tässä tutkimuksessa hylätään idealismin näkökulma, jonka mukaan vain ihmismielen mentaaliset ideat ovat tiedonlähteitä ja olioita ei ole olemassa ilman ihmismieltä (Tieteen termipankki 2019h). Sen sijaan tässä tutkimuksessa hyväksytään keskeiseksi ontologiseksi käsitykseksi emergentti materialismi, jonka mukaan yleisesti on olemassa vain materiaalisia olioita, joissa materian kasvava monimutkaisuus ja kehittyneisyys voi nostaa esille (engl. emerge) mentaalisia ominaisuuksia. Materialla onkin laadullisesti erilaisia tasoja, jotka monimutkaistuessaan synnyttävät uusia ominaisuuksia. Esimerkiksi ihmisellä ja eläimillä tällainen kehitys tapahtui aivojen toiminnan kehittyessä nykyiselle aistivalle ja ajattelevalle

tasolle evoluution tuloksena. Tietoisuus on hyvä esimerkki laadullisesta esille nousseesta ominaisuudesta, jota ei voida palauttaa suoraan materialistisiin alkutekijöihin. (Niiniluoto 1990; Niiniluoto 2001; Tieteen termipankki 2019f) Materialististen emergenttien olioiden ominaisuuksia eri kehitystasoilla käydään läpi tarkemmin teorialuvussa 4.

Tämän tutkimuksen näkökulma kybertilannekeskuksen ja muun tiedon tuottamiseen on empiristinen eli tutkimustieto perustuu kokemuksiin, havaintoihin ja tulkintaan – pelkän järkeilyn ja päättelyn eli rationalismin sijasta (Lähdesmäki ym. 2015, empirismi).

Epistemologiassa käsitellään tieto-opillisia eli tiedonsaantiin tai -tuottamiseen liittyviä periaatteita. Erityisesti tällä tieteenfilosofian osa-alueella ollaan kiinnostuneita menetelmistä, joilla tietämystä luodaan ja muodostetaan. Käytännössä nämä tarkoittavat käsityksiä pätevistä tutkimusmenetelmistä eli konkreettisista keinoista, joilla edellä kohdassa 2.1 esitettyyn tutkimuskysymykseen vastataan osuvimmin. Lisäksi epistemologiaan kuuluu tiedon, sen rinnakkaiskäsitteiden – esimerkiksi informaation – suhteiden määrittely, joka on esitetty tämän tutkimusraportin luvussa 3.2. (Hirsjärvi ym. 1997, 124-125) Jotta valinnat olisivat yhdenmukaisia ja tutkimustehtävän kannalta järkeviä, on niitä lähestytty tutkimustrategian eli tutkimuksen menetelmällisten ratkaisujen yhteensovittamisen näkökulmasta. (Lähdesmäki ym. 2015, interpretivismi)

Tässä tutkimuksessa epistemologinen **tutkimusstrateginen** valinta on interpretivistinen eli tulkinnallisuutta tiedon tuottamisessa korostava. Tämä tarkoittaa, että jo olemassa olevaa tutkimuskirjallisuutta ja tutkimuksen tiedonhankintamenetelmiä lähestytään tutkijan tulkinnan kautta, tarkkojen ja eksaktien tutkijan objektiivisuutta korostavien positivististen ajattelumallien sijasta. Valinta johtuu kyberturvallisuuden luonteesta tutkimuskohteena, jossa korostuvat kompleksisuus, kytkeytyneisyys ja avoimuus. Kybertilannekeskuksista saatava tieto piilee organisaatioiden rakenteissa, vuorovaikutussuhteissa ja ihmisissä, jolloin sen löytäminen vaatii tutkijan aktiivista roolia ja ihmisten tulkintaa. Tällöin tutkimuksen tavoitteeseen päästään parhaiten tulkinnallisten tieteenfilosofisten valintojen avulla.

Hermeneuttisen tutkimusstrategian mukaisesti tämä tutkimus on metodologisesti luonteeltaan kvalitatiivinen eli laadullinen. Edellisen lisäksi interpretivistinen tieteenfilosofinen valinta tukee hyvin laadullista tutkimusta (Lähdesmäki ym. 2015, interpretivismi). Kybertilannekeskuksesta ja organisaatioiden kyberresilienssiin vaikuttavista tekijöistä kerättävä

tieto on käytännössä todellisen elämän kuvaamista suhteineen ja ominaisuuksineen kokonaisvaltaisesti eli holistisesti. Samalla on tunnistettu, että tutkija vaikuttaa tutkimuksen tulokseen tulkinnoillaan ja arvoillaan, sillä tutkijaa ja tutkimuskohdetta ei voida laadullisessa tutkimuksessa erottaa toisistaan. Esimerkiksi teemahaastatteluissa tutkittavan ja tutkijan suhde on läheinen ja vapaa. Laadullisen tutkimuksen tekeminen on perusteltua, sillä kybertilannekeskustoiminta ja kyberturvallisuuden takaaminen ovat luonteeltaan kokonaisvaltaista ja moniulotteista toimintaa. Lisäksi tutkimusaiheen määrällinen eli kvantitatiivinen mittaaminen olisi ollut laajuuden ja moniulotteisuuden vuoksi vaikeaa. (Hirsjärvi ym. 1997, 131 ja 160-161) Tämä ei kuitenkaan estä määrällisten mittareiden kehittämistä tulevissa tutkimuksissa.

Aineistollisesti tämä tutkimus perustuu kyberturvallisuuden asiantuntijoiden puolistrukturoituihin kvalitatiivisiin teemahaastatteluihin ja olemassa olevaan teoreettiseen ja empiiriseen tutkimuskirjallisuuteen sekä muihin empiirisiin kirjallisiin lähteisiin.

Teemahaastatteluiden avulla on pystytty keräämään hiljaista tietoa kybertilannekeskusten toiminnasta – antamaan asiantuntijalle mahdollisuus puhua vapaammin – ja samaan aikaan ohjata tiedonkeruuta teemojen ja kysymysten avulla. Teemahaastattelut on valittu tiedonkeruumenetelmäksi, sillä kybertilannekeskusten vaikutuksista on vähän aiempaa tutkimusta ja ne ovat yleisesti ilmiöinä melko uusia ja tuntemattomia. (Saaranen-Kauppinen & Puusniekka 2006, teemahaastattelu) Puolistrukturoitujen teemahaastattelujen analysoinnista ja toteutuksesta on kerrottu tarkemmin luvussa 6.1.

Tutkimuskirjallisuus on koostunut vertaisarvioiduista tieteellisistä julkaisuista, artikkeleista, tutkimuksista ja kirjoista. Lisäksi monia verkkosivustoja ja uutisia on hyödynnetty esimerkkien tuottamisessa. Kaikkien kirjallisten lähteiden läpikäymisessä on noudatettu lähdekritiikkiä, joka on näkynyt esimerkiksi kirjoittajan tunnettuuden arvioinnissa, lähteen uskottavuudessa sekä lähteen iän ja alkuperäisyyden tarkastelussa (Hirsjärvi ym. 1997, 105-106). Sekundäärilähteitä on pyritty välttämään tiedon muuntumisen vuoksi, jolloin lähteinä on käytetty vanhempia primäärilähteitä. Tutkimusprosessin alussa on kattavan kokonaiskuvan saamiseksi toteutettu kirjallisuuskatsaus tutkimusaiheen tieteellisistä julkaisuista.

2.4 Teoreettinen tausta ja päättelymallit

Monitieteiseltä turvallisuuden tutkimukselta odotetaan moniparadigmaattisuutta ja tieteenalojen välisten ja sisäisten siilojen madaltamista (Virta 2012, 122-124). Tästä syystä tutkimuksessa on sovellettu rationaalisten paradigmojen joukkoon lukeutuvaa monitieteistä **järjestelmäteoriaa** ja sen suuntauksia. Järjestelmäteoria korostaa kontingentin eli tilannesidonnaisen lähestymistavan tarpeellisuutta organisaation toiminnassa. Lisäksi teoria kuuluu rationaalisen käsityksen piiriin, jossa organisaatiot nähdään osiensa kautta tarkasteltavina ja muunneltavina järjestelminä. Organisaation ohjaaminen tiettyyn suuntaan tapahtuu järjestelmää muuttamalla, jossa työntekijät toimivat asiantuntevasti ja laskelmoivasti. Rakenneanalyyttinen paradigma korostaa organisaation rakenteiden yhteensopivuutta, kontingenssia eli tilannesidonnaisuutta ja jatkuvan muutoksen tarpeellisuutta. (Guillén 1994; Seeck 2008, 35-37; Tieteen termipankki, 2019r)

Kvalitatiivisessa tutkimuksessa teorian ja tutkimuksen suhde voidaan nähdä teoriaa luovana – teorian varmistamisen sijasta (Hirsjärvi ym. 1997, 131). Tämän tutkimuksen teoreettisen taustan luo rakenneanalyyttiseen paradigmaan kuuluva järjestelmäteoria, jota sovelletaan ja muunnellaan kybertilannekeskuksen ja organisaatioiden kyberresilienssin kontekstiin. (Guillén 1994; Seeck 2008, 36-37). Järjestelmäteoria on valittu keskeiseksi teoriataustaksi, sillä se tukee kokonaisvaltaista eli holistista ajattelutapaa, avoimia järjestelmiä ja järjestelmien välisten suhteiden – vaikutusten – tutkimusta (von Bertalanffy 1968, 39, 44-45 ja 66).

Järjestelmäteoriaa on aikaisemmin sovellettu organisaatiotutkimuksessa etenkin palautteen perusteella tasapainoiseen tilaan pyrkivien ja mukautuvien kyberneettisten järjestelmien tutkimiseen, joista tässä tutkimuksessa sovelletaan erityisesti Bouldingin kompleksisuushierarkiaa (Boulding 1956; Seeck 2008, 161-162). Edellä mainittu mukautumiskyky on yksi organisaation kyberresilienssiin vaikuttavasta kolmesta keskeisestä osa-alueesta tilannetietoisuuden ja haavoittuvuuksien hallinnan lisäksi (Seville, Brunsdon, Vargo & McManus 2008, 82). Järjestelmäteoriaa täydennetään useilla teoreettisilla artikkeleilla organisationaalisesta resilienssistä ja tilannetietoisuudesta (Burnard & Bhamra 2011; Endsley 1995; Pettit, Fiksel & Croxton 2010; Seville ym. 2008). Valitun teoreettisen viitekehyksen sisältöä tarkastellaan tarkemmin luvussa 4.

Logiikassa on kyse tiedon toteen näyttämisen periaatteiden valinnasta ja perustelusta eli päättelymalleista (Hirsjärvi ym. 1997, 124). Kvalitatiivinen tutkimus – kuten tämäkin tutkimus – on tyypillisesti päättelymalleiltaan induktiivista (Halfpenny 1979, 799; Hirsjärvi ym. 1997, 133). Induktiivinen päättely tarkoittaa tietoa lisäävää päättelyä, joka yksittäistapauksessa merkitsee päättelyä yksittäistapauksesta yleistykseen. Induktiivisesti ajatellen tässä tutkimuksessa suoritetut teemahaastattelut ja aineistonkeruu voidaan yleistää kaikkiin kybertilannekeskuksiin. Tämän logiikan huonona puolena on, että johtopäätöksen paikkansapitävyydestä eli kybertilannekeskusten vaikutuksista organisaatioiden kyberresilienssiin ei voida olla täysin varmoja. Tätä ilmiötä kutsutaan induktion ongelmaksi. Tästä huolimatta induktiivisia yleistyksiä pidetään tiedepiireissä hyvin hyödyllisinä ja ne ovat tieteessä muutoinkin yleisiä. Asia tulee kuitenkin tunnistaa tarkasteltaessa tutkimustulosta. (Tieteen termipankki 2019i)

Hermeneutiikka – jonka mukaisesti tämän tutkimuksen tutkimusstrategia on valittu – tarkoittaa oppia ja filosofista suuntausta tutkimustekstien tulkinnasta, jossa pyritään ymmärtämään alkuperäisten tekstien kirjoittajien ympäristöä ja suhdetta kulloisenakin aikana vallinneisiin arvoihin ja yhteiskunnalliseen tilaan. Hermeneutiikassa korostetaan, että tekstien tulkinta on aina aikakautensa tulosta ja tapahtuu hermeneuttisen kehän lailla tekstin ja sen tulkitsijan välisenä dialogina, eikä lopullista tulkintaa ole olemassakaan. Tavoitteena on kasvattaa ymmärrystä tulkitsijan eli tutkijan ja tutkimustekstien välillä. (Gadamer & Linge 1977; Tieteen termipankki 2019g) Tästä syystä tässä tutkimuksessa käsiteltäviä teorioita ja empiirisiä ilmiöitä tarkastellaan nykypäivän kontekstissa soveltaen, vaikka monet teorioista ovatkin jopa yli 50 vuotta vanhoja ja nykypäivän empiiriset ilmiöt hyvinkin uusia ja tuoreita.

2.5 Tutkimusraportin rakenne

Tutkimusraportin ensimmäisessä osassa (**luku 1**) johdatellaan lukija tutkimuksen aihealueeseen kyberpoikkeamaesimerkein vuodesta 2006 tähän päivään. Toisessa osassa (**luku 2**) käydään läpi tutkimuskysymys kohta kohdalta, tutkittavan kohteen rajaus ja rajausten syyt, tieteenfilosofiset ja menetelmälliset aineiston hankintaan liittyvät valinnat, teoreettisen viitekehyksen valinnan perustelut ja tutkimusraportin rakenne.

Kolmannessa osassa (**luku 3**) käsitellään tutkimuksen kannalta keskeisten käsitteiden määrittelyt ja taustat. Neljännessä osassa (**luku 4**) käsitellään tutkimuksen teoreettinen viitekehys rakenneanalyyttiseen systeemiteoriaan ja kybernetiikkaan pohjautuvien suuntausten avulla. Tässä osassa esitellään lisäksi tätä tutkimusta varten kehitetty kybertilannekeskuksen resilienssimalli.

Viidennessä osassa (**luku 5**) käsitellään tutkimuskohteen eli kybertilannekeskuksen keskeiset empiiriset ominaisuudet tutkimuskirjallisuuden ja teemahaastatteluaineistosta saatujen kokemusten perusteella. Tutkimusraportin kuudennessa osassa (**luku 6**) raportoidaan asiantuntijoille tehtyjen teemahaastatteluiden toteuttamisen vaiheet ja aineiston analysointiin liittyvät seikat. Asiantuntijoiden kommentteja esitetään sitaateittain analysoiden.

Seitsemännessä osassa (**luku 7**) käsitellään tutkimuksen tuloksia eli kybertilannekeskusten vaikutusta organisaatioiden kyberresilienssiin ja pohditaan teoreettisen viitekehyksen yhteensopivuutta tutkimustuloksen kanssa. Luonnollisesti vastataan myös siihen, mitkä tekijät vaikuttavat organisaatioiden kyberresilienssiin. Kahdeksannessa osassa (**luku 8**) esitetään tutkimuksen johtopäätökset, jatkojalostetaan tutkimustuloksia ja esitetään arvio tämän tutkimuksen yhteiskunnallisesta ja tieteellisestä arvosta. Lisäksi esitellään tutkimusprosessin aikana ilmenneitä jatkotutkimuskohteita.

Tutkimusraportin lopussa on esitetty käytetyt lähteet hyvän tieteellisen käytännön mukaisesti. Liitteisiin on sisällytetty muun muassa asiantuntijahaastatteluissa käytetty teemahaastattelurunko ja käsitekartta.

3 KÄSITTEET JA TAUSTA

Käsitteet ovat ajattelun perusyksiköitä, jotka luovat ymmärryksen perustan ja kokoavat tietoa yhtenäiseksi jäsentyneeksi kokonaisuudeksi (Tieteen termipankki 2019j). Tässä luvussa esitetään tutkimuksen keskeisten käsitteiden määrittelyt, jotta tutkimusraportin kirjoittajan ja lukijan ajattelun perusta on mahdollisimman yhtenäinen. Monia tässä tutkimuksessa käytettäviä uuden teknologian ja verkottuneen maailman käsitteitä käytetään arkipäiväisessä kielenkäytössä vapaamielisesti, osittain ristiriitaisesti ja ilman kunnollista asemointia. Harvemmin kiinnitetään huomiota käsitteiden historiallisiin taustakytkentöihin ja niiden aiheuttamiin ajattelutapojen eroihin eri ihmisten välillä. Tästä syystä tässä tutkimuksessa on pyritty kiinnittämään erityistä huomiota käsitteiden määrittelyihin. Luku aloitetaan ”kyber”-käsitteen taustakytkentöihin ja historiaan tutustumalla.

3.1 Kyberin lyhyt historia – antiikista tähän päivään

Antiikin kreikkalainen filosofi Platon (noin 429-347 e.a.a.) on yksi tunnustetuimmista länsimaisen filosofisen kirjallisuusperinteen kirjoittajista (Kraut 2004). Hänen opettajanaan toimi merkittävä, puoleensavetävä ja arvoituksellinen filosofi Sokrates (noin 469-399 e.a.a.), joka nykytiedon valossa pyrki saamaan ihmisiä ja oppilaitaan, kuten Platonia, ajattelemaan itsenäisesti (Kraut 2004; Nails 2005). Tarkastelun kohteena olevan ”kyber”-käsitteen kannalta Platon on merkittävä henkilö. Etuliitteen ”kyber” muinaiskreikankielinen alkumuoto **κυβερνᾷ** (lausutaan *kyberna*, engl. ”to be a helmsman”, ”steer” ja ”govern”) on todennäköisesti peräisin Platonin teoksen *Valtio* teoskokoelman kirjasta numero yksi noin vuodelta 360 e.a.a. (Plato, Steadman & Burnet 2012, 12)

Platon käyttää teoksessaan merenkulun navigoinnista antiikin aikana käytettyä sanaa **κυβερνᾷ** (kyberna) tarkoittamaan laivan ohjaamisen sijasta yleisesti asioiden ohjaamista, hallintaa ja hallitsemista. Ajan saatossa sana muuttui muotoon *kybernetes* (engl. steersman, helmsman), joka tarkoittaa laivan ruorimiehenä olemista. Sana *kybernetes* on toiminut kantasanoina myös englannin kielen sanoille hallita ”govern” (kreik. κυβερνώ eli kubernó) ja olla kuvernööri ”governor” (kreik. κυβερνήτης eli kubernḗtēs) (Beynon-Davies 2011, 78; Glosbe 2019). Tämä tekee sanan historiasta erityisen mielenkiintoisen hallintotieteellisestä näkökulmasta.

Alun perin sana **κυβερνᾷ** (kyberna) on todennäköisesti ollut jo antiikin kreikkalaisen runoilijan Pindaroksen (noin 520 – 440 e.a.a.) runoissa käyttämä, sillä Platon viittaa Pindarokseen käyttäessään kyberna-sanaa kirjassaan.

Käännös suomeksi:

Kauniisti, oi Sokrates, hän [Pindaros] *sanoi: se ken elämänsä elää oikeudenmukaisesti ja hartaasti, on tuleva elämään täynnä suloista toivoa, tuota ikuista sielun hoitajaa ja matkakumppania. Toivoa, joka useimmiten* ***ohjaa*** */* ***hallitsee*** *kuolevaisen vaihtelevaa sielunelämää.* (Pindarus & Sandys 1915, 608-609)

Alkuperäinen muinaiskreikaksi:

χαριέντως γάρ τοι, ὦ Σώκρατες, τοῦτ' ἐκεῖνος εἶπεν, ὅτι ὃς ἂν δικαίως καὶ ὁσίως τὸν βίον διαγάγῃ, "γλυκεῖά οἱ καρδίαν ἀτάλλοισα γηροτρόφος συναορεῖ ἐλπὶς ἃ μάλιστα θνατῶν πολύστροφον γνώμαν ***κυβερνᾷ****.* (Plato ym. 2012, 12-13)

Nykyään kyberin tulkinnasta on paljon erilaisia versioita ja merkityksiä eri konteksteissa, joista asiantuntijatkin ovat erimielisiä. Platonin tuotosten pohjalta voimme kuitenkin päätellä sen kantasanan tarkoittaneen alun perin jonkin asian ohjaajana olemista, hallitsemista tai hallintaa. Sanan ”kyber” kantasanan ”kyberna” tarkoituksen tunteminen on tärkeää, jotta voidaan ymmärtää sanan merkityksen muutoksia historiallisesti ja täsmentää sanan nykymerkitys.

Vuonna 1834 ranskalainen fyysikko, elektromagnetismin keksijä ja sähkövirran yksiköstä ampeerista tunnettu filosofi André-Marie Ampère (1775-1836) otti käyttöön käsitteen kybernetiikka (kreik. κυβερνετική, kubernetike). Kybernetiikka oli alun perin johdettu kreikankielisestä merkityksestä merellä kulkevan aluksen ohjaustaidolle, jonka Ampère sovelsi edelleen ”yleiseksi hallinnan taidoksi” (ransk. ”de l'art de gouverner en général”) (Shank 2019). Tämä tukee aiempaa havaintoa kyberin alkuperästä jo antiikin kreikan eli Platonin ajoilta. (Dyson 1997, 5)

Kauan ennen varsinaisen ”kyber” käsitteen tai etuliitteen olemassaoloa Ampère kirjoitti kirjoitelman ”*Tieteenfilosofiasta ja kaiken ihmisen tietämyksen luonnollisesta analyyttisen luokittelun tarkastelusta*”. Kirjoitelmassa listataan kolmenasteisia keinoja, joilla valtiot ylläpitävät turvallisuutta, järjestystä ja rauhaa. Yksi keinoista oli kybernetiikka (”Cybernétique”), jolla Ampère tarkoitti ”hallinnan taidetta” eli käyttäytymissääntöjä eri tilanteissa (”des règles

générales deconduite") ja toimenpiteitä ("mesures"), joiden pohjalta kansakuntaa tai organisaatioita hallitaan ("à la nation qu'il régit") ja ohjataan haluttuun suuntaan yksittäisillä päätöksillä ("qui le guident dans chaque cas particulier") – kuten merellä ajelehtiva laiva ohjattaisiin myrskyn jälkeen oikeaan satamaan. (Ampère 1834, § IV; Dyson 1997, 5)

Fyysikko Ampère ei ollut ainoa teknologisen kehityksen esikuva, vaan hieman hänen jälkeensä englantilainen Charles Babbage (1791-1871) kehitti ensimmäisen mekaanisen tietokoneen mallin – nimeltään analyyttisen koneen – ja kehitteli ajatuksen reikäkorttien avulla ohjelmoitavasta tietokoneesta (Hyman 1982, 243-245). Ideaa jatkojalosti 1840-luvulla englantilainen Ada Lovelace (1815-1852), joka tutki Babbagen muistiinpanoja ja kirjoitti analyyttiselle koneelle maailman ensimmäisen tietokoneohjelman (Fuegi & Francis 2003, 16).

Teknologinen kehittyminen oli nopeaa jo 1800-luvulla, mutta uusi vaihde kehityksen nopeuteen vaihdettiin toisen maailmansodan aikoihin, jolloin amerikkalainen John von Neuman (1903-1957) kehitti elektronisen tietokoneen toimintaperiaatteen ja brittiläinen Alan Turing (1912-1954) rakensi ohjelmoitavan digitaalisen tietokoneen sotilaallisiin tarpeisiin (Hodges 2012, 554; von Neumann 1945). Yhdessä edellä mainitut tapahtumat johtivat tiedepiireissä niin kutsutun rakenneanalyyttisen ajattelun voimistumiseen, jossa organisaatiot nähtiin rationaalisina järjestelminä, joiden osia, suhteita ja toimintaa voidaan tutkia täsmällisesti. Kybernetiikkaa pidetään nykyään edellä kuvatun järjestelmäteoreettisen ajattelun yhtenä ilmentymänä tai sivuhaarana. (Seeck 2008, 161-162)

Suuren yleisön tietoisuuteen kybernetiikka tieteenalana nousi, kun yhdysvaltalainen matemaatikko Norbert Wiener (1894-1964) kirjoitti 1940-luvun lopussa teoksensa "*Cybernetics or Control and Communication in the Animal and the Machine*". Teoksessa Wiener kertoo valinneensa tutkimusryhmänsä kanssa kreikan kielestä muodostuneen keinotekoisen uuden käsitteen *kybernetiikka* kuvaamaan uutta inhimillisten ja mekaanisten järjestelmien automaattiseen kommunikaatioon ja kontrolliin perustuvaa tutkimusalaa. Kybernetiikassa järjestelmät toimivat ulkoisen palautteen perusteella omaa toimintaansa säädellen ja mukautuen muuttuvaan toimintaympäristöön. (Lemak 2004, 1319; Wiener 1948, 11) Erikoisen Wienerin käsitevalinnasta tekee se, että Ampère käytti samaa käsitettä jo 1800-luvulla melko samanlaisessa merkityksessä. Toisaalta Ampère painotti kybernetiikan yhteiskunnallista ja hallin-

nallista ulottuvuutta, kun Wiener painotti toiminnan säätämistä muuttuvan toimintaympäristön mukaisesti. Joka tapauksessa Wiener on tunnetumpi ”kybernetiikka” käsitteestään. Wienerin kybernetiikkaa on käsitelty tarkemmin teoriaosuudessa luvussa 4.

Wienerin ja muiden kyberneetikkojen käyttäessä ”uutta” kybernetiikan (cybernetics) käsitettä tietojenkäsittelyn, biologian ja tekniikan aloilla, tuli käsitteelle suuren yleisön joukossa futuristinen konnotatiivinen sivumerkitys. Tällöin varsinainen lyhennelmä ”cyber” otettiin yleisemmin käyttöön mitä erilaisimmissa merkityksissä – myös tieteiselokuvien ja sarjojen osalta. Yksi esimerkki on kyborgi (engl. cyborg), jonka alkukirjaimet ”cyb ” tulee kybernetiikasta (engl. cybernetics) ja ”org” sanasta organismi (engl. organism) biologiasta. Kyborgi tarkoitti tässä yhteydessä ihmisen kaltaista konetta, jolla oli mahdollisuus mukautua itsenäisesti muuttuviin ympäristöihin. (Coe 2015)

Wienerin tieteellisestä uudesta käsitteestä tuli tieteiselokuvien ja -kirjojen osalta mitä erilaisimpia muunnelmia. 1980-luvulla tieteiskirjailija William Gibson kirjoitti teoksensa ”Burning Chrome”, jossa kaksi freelancer-hakkeria pyrkii tunkeutumaan rikollispomo Chromen tietojärjestelmiin kyberavaruudessa (Gibson 1986a, 176). Mainitussa teoksessa esiintyy käsite kyberavaruus (engl. cyberspace) tiettävästi ensimmäistä kertaa koskaan. Wiener selventää myöhemmin ilmestyneessä teoksessa ”Neuromancer” kyberavaruuden käsitteen olemusta seuraavasti: *kaikkien ihmisten yhteisenä kaikkea tietoa graafisesti kuvaavana äärimmäisen kompleksisena hallusinaationa, joita miljardit ihmisoperaattorit katselevat jokaisessa maassa* (Gibson 1986b, 44). Jo tuolloin kyberavaruuden määritelmässä yhdistyivät ihmisen havainnointikyvykkyyden tärkeä rooli ja ympäristön äärimmäinen kompleksisuus. Kyberavaruuden käsitettä alettiin käyttää nopeasti myös tieteellisissä julkaisuissa. (Coe 2015; Rain Ottis & Peeter Lorents 2010, 267)

Viime aikoina kybernetiikasta juonnettua kyberiä on käytetty kuvaamaan lähes mitä tahansa virtuaalitodellisuuteen, tietojenkäsittelyyn ja tietoverkkoihin, kuten internetiin, liittyvää asiaa. Se toimii yleisesti etuliitteenä ja omana sananaan. (Merriam-Webster 2019a; Oxford University Press 2019; Rain Ottis & Peeter Lorents 2010, 267)

Tässä tutkimuksessa kyberin määritelmässä yhdistetään Platonin, Ampèren ja Wienerin näkökulmat nykypäivän ajattelutapojen kanssa.

3.2 Käsitteet

Tässä alaluvussa kuvataan tutkimuksen kannalta keskeiset käsitteet. Määritelmissä pyritään kuvaamaan käsitteen olemus, välttämään kehämääritelmiä, positiiviseen määritelmään negatiivisen sijasta – mitä käsite ei tarkoita – ja syntaktisesti oikeaan kielenkäyttöön. (Niiniluoto 1997, 164) Kybertilannekeskuksen määritelmä on turhan toiston välttämiseksi kuvattu erikseen kybertilannekeskustoiminnan empirialuvussa 5.

3.2.1 Kyberiin liittyvät käsitteet, turvallisuus ja resilienssi

Kyber tarkoittaa tässä tutkimuksessa asioiden tai esineiden – järjestelmien – laatua (adjektiivi), joita voidaan ohjata ja hallita automaattisen kommunikaation (viestintä) ja kontrollin (säätö) avulla. Kyberasioiden automaattisen viestinnän ja säätelyn menetelmiä ja välineitä kutsutaan tieto- ja viestintäteknologiaksi eli **tietotekniikaksi**. Täysin ilman tietotekniikkaa toteutettava kommunikaatio ja kontrolli eivät kuvaa tässä tutkimuksessa kyberominaisuuksia omaavia järjestelmiä.

Ohjaaminen ja hallitseminen tapahtuu edellä mainittujen kyberasioiden muodostamassa aikariippuvaisessa, verkostomaisessa ja kompleksisessa tietoteknisessä ympäristössä eli **kyberavaruudessa**. Internet ja muut verkottuneet tietotekniset järjestelmät sekä näiden kanssa vuorovaikuttavat (kommunikaatio) ja niitä ohjailevat (kontrolli) järjestelmät – esimerkiksi ihmiskäyttäjät – muodostavat kyberavaruuden kokonaisuuden. Ihmiskäyttäjillä tarkoitetaan ainoastaan ihmisestä lähtöisin olevaa vuorovaikutusta ja ohjausta esimerkiksi tietokoneen käyttöliittymän tai selaimen välityksellä – ihminen ei itse ole osa kyberavaruutta, vaan sen vaikutusympäristöä. Järjestelmät, jotka toimivat täysin ilman suoraa kytkentää tietotekniikkaan eivät kuulu kyberavaruuteen. Kyberavaruus on ihmisen luoma rajallinen, keinotekoinen ja jatkuvasti muuttuva laaja tietotekninen vuorovaikutuksen välittäjäverkosto. (International Organization for Standardization 2012, 4.21; Rain Ottis & Peeter Lorents 2010, 268)

Aikariippuvuus – kyberavaruuden ominaisuutena – tarkoittaa kyberavaruuden rakennuspalikoiden eli elementtien ja niiden välisten suhteiden jatkuvaa erittäin nopeaa muutoksen mahdollisuutta ajan – eli jatkuvan ja peruuttamattoman menneisyydestä nykyhetken kautta tulevaan etenevän prosessin – suhteen (Merriam-Webster 2019c; Read 1999, 1314). **Verkostomaisuus** tarkoittaa kyberavaruuden elementtien yhteyksiä ja vuorovaikutusta toisiinsa.

Esimerkiksi erilaiset siirtotiet kaapelit ja radioyhteydet sekä internetin palvelut, linkit ja nimipalvelujärjestelmät (DNS) yhdistävät tietoteknisiä toimintoja yhtenäiseksi toiminnalliseksi verkostoksi. **Kompleksisuudella** (lat. complexus = yhteen kudottu) viitataan kyberavaruuden monien elementtien vuorovaikutuksesta aiheutuvaan keskinäisriippuvuuteen eli osien välisiin vaikeasti hahmotettaviin vaikutuksiin. Kompleksisuuden muodostavat ihmiskäyttäjien määrä, verkoston laajuus ja jatkuva muutos, joiden syy-seuraussuhteita on vaikea etukäteen havaita. (Rain Ottis & Peeter Lorents 2010; Tieteen termipankki 2019b)

Kyberillä kuvattavia ominaisuuksia omaavien järjestelmien vaikutukset, uhat ja mahdollisuudet tapahtuvat **kyberavaruuden vaikutusalueella**, joka sisältää koko tietoteknisen kyberavaruuden ja sen ulkopuolisen fyysisen ja inhimillisen vaikutusalueen. Toisin sanoen kyberavaruuden vaikutusympäristössä voi olla täysin ilman tietotekniikkaa toimivia järjestelmiä – esimerkiksi ihmisiä – johon kyberavaruus kuitenkin välillisesti vaikuttaa uhkineen ja mahdollisuuksineen. (Rain Ottis & Peeter Lorents 2010, 268)

Turvallisuus tarkoittaa järjestelmän toimintaympäristössä olevien vahingollisten ja pakottavien muutosvoimien eli vaarojen ja uhkien poissaoloa tai hyvää sietokykyä eli resilienssiä. Toisin sanoen samassa järjestelmässä samaan turvallisuuden tasoon voidaan päästä vaarojen ja uhkien vähäisellä määrällä ympäristössä tai sillä, että niiden ilmaantuminen ei aiheuta juurikaan haittaa järjestelmän toiminnalle. Järjestelmä voi olla ihminen, organisaatio, kone tai mikä tahansa systeemi, jonka turvallisuuden tason ihminen tulkitsee.

Resilienssi (engl. resilience) tarkoittaa toimijan – esimerkiksi järjestelmän, organisaation tai osaston – kykyä suunnitella, vastata ja toteuttaa haluttua toimintaa jatkuvasti haitallisista muutosvoimista huolimatta. **Jatkuvuus** tarkoittaa kykyä kaikissa tilanteissa toipua ja palauttaa toiminta sidettävälle tai normaalia paremmalle tasolle. Jatkuvuuteen vaaditaan kyky palautua eli palauttaa, muuttaa tai muokata normaaleja toimintoja tilannevasteilla erilaisissa tilanteessa, jotta toimintojen jatkuvuus voidaan varmistaa. **Kyberresilienssi** (engl. cyber resilence) tarkoittaa kykyä jatkaa toimintaa haitallisista kyberavaruuden muutosvoimista huolimatta. (Björck, Henkel, Stirna & Zdravkovic 2015) Kyberresilienssiä käsitellään laajemmin luvuissa 4 ja 6.

Käsitteet **kybertilannekeskus**, kybertilannekeskuksen **edunsaaja** ja **kybertilannekeskustoiminta** määritellään erillisessä kybertilannekeskustoimintaa käsittelevässä luvussa 5.1.

Kyberturvallisuus (engl. cybersecurity) tarkoittaa kyberavaruudessa ja sen vaikutusalueella oleviin järjestelmiin kohdistuvien ihmisten vahingollisiksi ja pakottaviksi tulkitsemien muutosvoimien eli kyberuhkien poissaoloa ja hyvää sietokykyä eli kyberresilienssiä. Muutosvoimat aiheuttavat järjestelmien tulevalle toiminnalle epävarmuutta eli mahdollisuuksia ja haavoittuvuuksia, joita pyritään hyödyntämään ja torjumaan hallintakeinoilla. Hallintakeinot ovat organisaation kyvykkyyksiä (kuvio 1). Toisin sanoen kyberturvallisuus on ihmisen käsitys tietotekniikan vaikutusalueella tapahtuvan kommunikoinnin ja kontrolloinnin turvallisuuden tasosta (von Solms & van Niekerk 2013, 100-101).

Kyberturvallisuus kattaa kyberavaruudesta välittömästi muodostuvaa kommunikaation ja kontrollin turvallisuuskokonaisuutta laajemman osa-alueen, sillä kyberturvallisuuden piiriin kuuluvat lisäksi sellaiset välilliset asiat, jotka eivät suoranaisesti hyödynnä tietotekniikkaa, mutta ovat haavoittuvia tietotekniikasta aiheutuville uhkille. Tästä syystä kyberturvallisuus ei rajoitu vain tietoteknisten järjestelmien turvallisuuteen, vaan kattaa myös sen vaikutusalueen eli ympäristön turvallisuuden (von Solms & van Niekerk 2013, 100-101).

Tietoturvallisuus (engl. information security) tarkoittaa tiedon arvoketjun (määrittely luvussa 3.2.2) luottamuksellisuuden, eheyden ja saatavuuden turvaamista (vrt. kyberturvallisuus). *Luottamuksellisuus* tarkoittaa, että tiedon arvoketjun osat eivät ole saatavilla tai paljastuneet luvattomille henkilöille, tahoille tai prosesseille. *Eheys* puolestaan tarkoittaa, että tiedon arvoketjun osat ovat oikeellisia ja kokonaisia. *Saatavuus* tarkoittaa, että tiedon arvoketjuun on pääsy valtuutetulle käyttäjälle tarvittaessa. (International Organization for Standardization 2018, 3.28, 3.10, 3.36 ja 3.7)

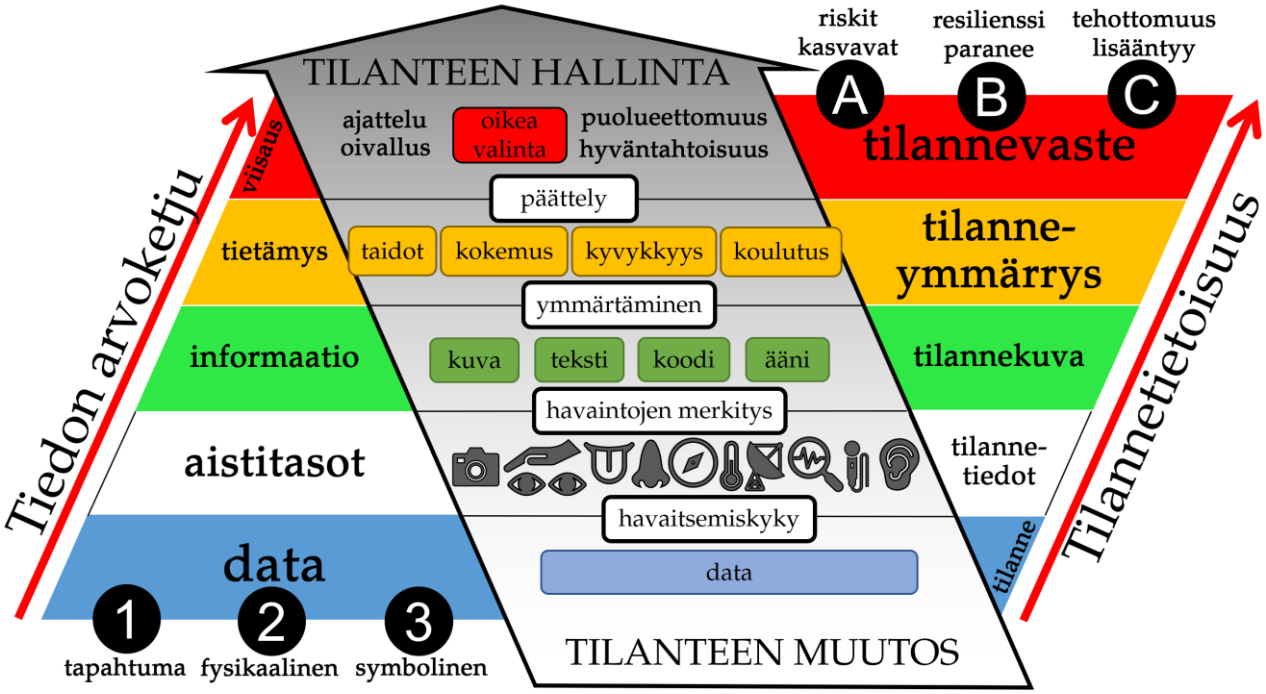
Kyberturvallisuus ja tietoturvallisuus ovat osittain päällekkäisiä ja osittain erillisiä käsitteitä, mutta kumpikaan käsitteistä ei sisällytä toistaan täysin itseensä. Kyberturvallisuus kattaa käsitteenä sen osan tietoturvallisuudesta, joka liittyy tietotekniseen eli sähköiseen tiedon arvoketjun turvallisuuteen. Kyberturvallisuus ei käsitä sellaista turvallisuutta, joka tallennetaan tai viestitään ilman tietotekniikkaa. Toisaalta tietoturvallisuus ei käsitä tiedon arvoketjuun (määritelty luvussa 3.2.2) liittymätöntä turvallisuutta. Tästä esimerkkinä ovat kyberavaruuden vaikutuspiirissä olevien järjestelmien fyysinen turvallisuus, rakennusten ja kotien turvallisuus sekä yhteiskunnan kokonaisvaltainen hyvinvointi ja toimintakyky. (von Solms & van Niekerk 2013, 99-101)

Käsitteiden näkökulmat ja kysymyksenasettelu ovat erilaiset, mutta osiltaan päällekkäiset:

1. Kyberturvallisuus: mitä tietotekniikalla voi saada aikaan (vaikuttaa) ympäristössä?
2. Tietoturvallisuus: mitä tietoja on käytettävissä (havaitseminen) ympäristöstä?

Tietotekniikka välittäjänä ja kommunikaatiokanavana on molemmille näkökulmille yhteinen turvallisuustekijä. Graafinen käsitekartta kyber- ja tietoturvallisuuden eroista on esitetty liitteessä 2.

3.2.2 Tiedon arvoketjun ja tilannetietoisuuden suhde



Kuvio 1. Tiedon arvoketjun (vasen pyramidi) ja tilannetietoisuuden (oikea pyramidi) käsitteistön suhde osana ympäristön muutosvoimien hallinnan prosessia (harmaa nuoli keskellä yläviistoon). Tieto jalostuu ja tilannetietoisuus paranee kuviossa alhaalta ylöspäin.

Tiedon arvoketju (kuvio 1) tarkoittaa neljästä käsitteestä koostuvaa DIKW-mallia, joka jäsentää ja asemoi: datan (engl. data), informaation (engl. information), tietämyksen (engl. knowledge) ja viisauden (engl. wisdom) käsitteet toistensa suhteen. (Ahsan & Shah 2006, 1-7)

Tilanne (engl. situation) (kuvio 1) tarkoittaa asioiden tilaa ja olemusta tietyssä ajassa ja paikassa. (Read 1999, 1176)

Tietoisuus (engl. awareness) (kuvio 1) on laadullinen todellisista tai virtuaalisista aistipohjaisista havainnoista koostuva *mekanismi*, joka muodostaa raportoitavissa olevan muistikuvan. Tietoisuuteen tarvitaan huomion kiinnittyminen kyseiseen asiaan – jos tätä asiaa ei

huomaa, ei siitä voi myöskään olla tietoinen. (Haikonen 2017, 202) Ihmisten lisäksi tietoisuutta on todistetusti eläimillä ja mahdollisesti myös kasveilla (Haikonen 2017, 205; Low 2012). Koneilla ei ole tietoisuutta, sillä tietoisuuden ilmenemiseen vaaditaan sosiaalista vuorovaikutusta kulttuuriympäristön kanssa, neuroverkkojen suurta ristiinkytkentöjen määrää ja siitä muodostuvaa emergenssiä. Koneet eivät ymmärrä, koska koneilla ei ole itsetietoisuutta (Niiniluoto 1990, 132-135). Tietoisuuden tarkka syntymekanismi ja selitys on laajan filosofisen ja tieteellisen debatin kohteena. Tässä tutkimusraportissa esitettävä näkemys on yksi monista esillä olleista tietoisuuden määritelmistä. (Haikonen 2017, 198)

Tilannetietoisuus (engl. awareness) (kuvio 1) tarkoittaa kognitiivisen tiedon järjestäytymistä eli tietoisuuden aistisisällön eli kvalian (engl. qvalia) olemassaoloa (Haikonen 2017, 198). Tietoisuusmekanismin pohjalta tiettyyn aikaan ja paikkaan eli *tilanteeseen* liittyvä *havainto*, siitä tehdyt *merkitysten tulkinnat* ja *ymmärrys* sekä näiden pohjalta tehtävät *päätökset* eli päätellyt *vasteet* tilanteeseen muodostavat tilannetietoisuuden (kuvio 1) tietoisen kokemuksen. Jokaisella edellä mainitulla tasolla voi syntyä **havaitsemisharhoja**, jotka vaikuttavat tilannetietoisuuden oikeellisuuteen. (Åhman & Rauhala 2017, 117; Kokar & Endsley 2012)

Data (monikko, engl. data) (kuvio 1) tarkoittaa otaksuttuja tosiasioita, tosiseikkoja tai tosioita (yksikkö *tosio*, engl. datum) tietyssä **tilanteessa** esiintyvien erojen tai yhtenäisyyden puuteen vuoksi. Toisin sanoen, yksi **tosio** on kokonaisuus, joka esittää poikkeaman. Vähintään kaksi tosiota muodostaa datan. Tosio voidaan havaita kolmella tavalla näkökulmasta riippuen. Yhtenäisyyden puutteena (kuviossa 1 mustilla palloilla numeroituna) …

- todellisen maailman kohteessa (lat. de re) eli **tapahtumana** ”luonnossa”.
- kahden **fysikaalisen** (lat. de signo) tilan välillä. Esimerkiksi hiljainen tai kova ääni.
- kahden **symbolin** (lat. de dicto) välillä. Esimerkiksi symbolit $ tai € sekä 1 tai 0.

Todellisuudessa esiintyvä tilanne eli (1) ”tapahtumien virta” on identtinen tai mahdollistaa (2) fysikaalisen tosion havaitsemisen, joka puolestaan mahdollistaa tosion (3) symboliksi koodaamisen. (Luciano & Zalta 2019; Niiniluoto & Hallinnon kehittämiskeskus 1996, 27-30)

Havaitseminen (engl. perception) tai **havaitsemiskyky** (engl. sentience) (kuvio 1) tarkoittaa kykyä ottaa vastaan ärsykkeitä eli stimulaatioita aistikanavien tai sensoreiden eli modaliteettien avulla (English Oxford Living Dictionaries 2019b). Tiettyyn ajallisesti ja paikallisesti

rajattuun tapahtumaan liittyvistä stimulaatioista käytetään nimitystä **tilannetiedot**. Esimerkiksi ihmisen suoria havaitsemisen mahdollistavia aistikanavia ovat maku-, kuulo-, haju-, näkö- ja tuntoaisti (Yle Oppiminen 2015). Ihmiseltä puuttuvia suoria aistikanavia ovat muun muassa kalojen sähkö- ja magneettikenttäaisti, lepakoiden ja käärmeiden infrapunaaisti sekä tarkka haju- ja kuuloaisti (Keeley 2015, 2-3). Myös kasveilla on monia aisteja, kuten valo, lämpötila ja painovoima-aisti (Chamovitz 2012, 9, 49 ja 91). Koneiden ja laitteiden aisteja kutsutaan **antureiksi** (engl. sensor). Anturi muuttaa mitatun muuttujan - esimerkiksi jännitteen, taajuuden, säteilyn, kiihtyvyyden tai ajan – sähköiseksi signaaliksi tiedonsiirtoa varten (Tieteen termipankki 2019a). Anturi voi myös mitata jo valmiiksi sähköistä signaalia ja muuttaa sen haluttuun tulkittavaan muotoon. Tällaiset anturit mahdollistavat kyberavaruuden tapahtumien havaitsemisen (lisää luvussa 5.5).

Havainto (engl. observation) puolestaan tarkoittaa tapahtumaa, jossa **havainnoija** (engl. observer) käsittelee havaitsemiskyvyn avulla jonkin stimulaation (English Oxford Living Dictionaries 2019a). Havainnoija on tyypillisesti elävä olento, kuten ihminen, mutta ihminen voi myös ohjelmoida koneen havaitsemaan haluttuja asioita esimerkiksi kyberavaruuden muutoksista. Havainnot tapahtuvat järjestelmistä koostuvassa **havainnointiavaruudessa** (engl. space of observation) – kuten kyberavaruudessa – aistitason havaitsemiskyvyn kautta. Ilman aistitasoa havaitseminen, havaintojen tekeminen ja niiden merkitysten tulkitseminen ei ole mahdollista. (Luciano & Zalta 2019)

Aistitasot (engl. levels of abstraction) (kuvio 1) ovat aisteista, sensoreista ja aistien käsittelystä muodostuneita järjestelmien liittyntäpintoja, jotka mahdollistavat muista järjestelmistä tehtävät havainnot, havaintojen merkityksen tunnistamisen ja niiden muuttamisen informaatioksi. Aistitason ominaisuudet määrittelevät datan laajuuden ja tyypit, joihin havainnoijalla on havaitsemismahdollisuus eli pääsy. Aistitaso yhdistää havainnoijan ja havainnoinnin kohteen. Näin ollen aistitaso on ikään kuin näkökulma, jolla havainnoija havainnoi kohdetta. Aistitasolla havaitut tosiseikat eli data rajoitettuine käyttömahdollisuuksineen muunnetaan semanttiseksi eli merkityssisältöiseksi ja kontekstisidonnaiseksi informaatioksi. (Luciano & Zalta 2019; Read 1999, 873)

Havainnoija ei voi tehdä havaintoa ilman aistitasoa, sillä havaitseminen ei voi kohdistua koskaan suoraan tosiseikkoihin tai dataan ilman liityntäpintaa havainnointiavaruuden järjestelmiin. Toisin sanoen, ilman aisteja ja niiden käsittelyä ei voi havainnoida ympäristöä.

Lisäksi aistitason laajuus ja monipuolisuus datan vastaanottamiseksi vaikuttavat informaation pätevyyteen. Esimerkiksi kyberavaruudesta saatavan datan laatu ja kattavuus perustuvat aistitasojen tarjoamiin mahdollisuuksiin, jotka vaikuttavat suoraan datasta muodostettavan informaation laatuun ja käytettävyyteen. (Luciano & Zalta 2019; Read 1999, 873)

3.2.3 Informaation yleinen määritelmä ja tilannekuvan ominaisuuksia

Informaatio koostuu (1) yhdestä tai useammasta (2) hyvin muotoillusta (3) merkityssisältöisestä tosiseikasta eli datasta (kuvio 1).

1. ”*Koostuminen yhdestä tai useammasta tosiseikasta eli datasta*” tarkoittaa, että informaatiota ei voi olla ilman dataa eli havaittuja tosioita tai tosiseikkoja. Yksinkertaisimmassa tapauksessa informaatio koostuu yhdestä havaitusta tosiseikasta.
2. ”*Hyvin muotoiltu*” tarkoittaa, että data on ryhmitelty yhteen syntaksisääntöjen mukaisesti. Syntaksisäännöt määräävät valitun järjestelmän, jolla data analysoidaan: koodaus, kieli tai muu järjestelmä. Tämä järjestelmä voi olla muoto, rakenne, koostumus tai jäsennys jostakin, ei ainoastaan kielitieteellinen asia. Tästä esimerkkinä vaikkapa tavallinen kuva, äänite tai koodattu sanoma.
3. ”*Merkityssisältöinen*” tarkoittaa, että datan on sisällytettävä valitulla syntaksisäännön mukaisella järjestelmällä tuotettua kontekstisidonnaista tulkittavaa merkityssisältöä eli semantiikkaa. Näin ollen informaatiota ei esiinny ”luonnossa”, vaan se on aina älykkään tuottajan datasta muokkaamaa tulkintaa kontekstisidonnaisesti.

Merkityssisältö voi olla tosiasiallista (engl. factual) tai opastavaa (engl. instructional). (Luciano & Zalta 2019)

Tosiasiallinen merkityssisältö tarkoittaa semanttista informaatiota, joka voi olla totta tai epätotta. Tosiasiallisella informaatiolla on datan luonteesta johtuvia *rajoitteita* (engl. constraints) ja *käyttömahdollisuuksia* (engl. affordances). Datan havainnoija voi ottaa käyttöön tai rajoittaa datan käyttöä – eli säätää ja hallita datan prosessointia – perustuen vuorovaikutussuhteen laatuun ja havainnoijan olemukseen. Tässä mielessä saatavilla olevan datan laatu rajoittaa, mahdollistaa ja on merkittävässä asemassa tosiasiallisen informaation tuottamisessa. Esimerkiksi kyberhyökkäyksen havaittu alkamiskellonaika on informatiivinen tosiasiallinen mahdollisuus, jos voidaan olla datan perusteella varmoja, että hyökkäys

todella on alkanut silloin (rajoite). Tosiasiallinen informaatio mahdollistaa tilanteen tasalla olemisen. (Luciano & Zalta 2019)

Opastava merkityssisältö tarkoittaa informaatiota, jota ei voida määritellä todeksi tai epätodeksi. Opastava informaatio ei kuvaa tilannetta, vaan se kuvaa ehtolauseilla, miten jokin ilmiö saadaan aikaiseksi. Esimerkiksi poikkeamatilanteita varten tehdyt toimintaohjeet, määräykset ja prosessikuvaukset eli **varautuminen** ja varautumissuunnittelu ovat informaationa opastavia ja niiden käyttäminen vaatii tulkintaa. Opastavalla merkityssisällöllä varustettu informaatio sisältää esimerkiksi kyberuhkien hallintakeinoja ja mahdollistaa kyberresilienssin parantamisen. (Luciano & Zalta 2019)

Tosiasiallinen ja opastava informaatio yhdessä mahdollistavat tilannekuvan syntymisen. **Tilannekuva** (kuvio 1) on jokaisen ihmisen itse muodostama subjektiivinen kuva, käsitys ja tulkinta vallitsevasta tilanteesta ja sen merkityksestä. Kun tilannekuva on jaettua ja kaikki käsittävät tilanteen samoin, voidaan puhua **jaetusta tilannekuvasta**. **Kybertilannekuva** muodostetaan kyberavaruuden havaintojen perusteella.

Vääräksi informaatioksi (engl. misinformation) kutsutaan informaatiota, jonka semanttinen sisältö on epätotta. Sen sijaan, jos informaation lähde on tahallisesti muodostanut väärää informaatiota, on kyseessä **harhaanjohtava informaatio** eli disinformaatio. (Luciano & Zalta 2019) Väärä tai harhaanjohtava informaatio saattavat johtaa virheelliseen käsitykseen todellisuudessa vallitsevasta tilanteesta.

3.2.4 Tiedon arvoketjun korkeimmat tasot ja päätöksenteko

Ymmärtäminen (engl. understanding) (kuvio 1) tarkoittaa tulkitsijan elämänkäytännön ja aikakauden ajattelutapojen kautta tapahtuvaa totuuden kokemisen prosessia. Ymmärrys pohjautuu merkitykselliseen (semanttiseen) *tosiasialliseen* (mitä tapahtuu) ja *opastavaan* (miten toimia) informaatioon. Ymmärrys muuttaa informaation tietämykseksi. Ymmärrys tapahtuu prosessimaisesti hermeneuttisen kehän avulla, jossa ymmärrys informaation taustalla olevasta ilmiöstä syvenee vähitellen vuoropuheluna tulkitsijan ja kohteen välillä. (Tieteen termipankki 2019o)

Tietämys (engl. knowledge) (kuvio 1) tarkoittaa tilannetta, jossa informaatio on yhdistetty kokemuksen ja koulutuksen kautta hankittuihin kykyihin ja taitoihin ymmärtämisen avulla

(Read 1999, 706). Tietämyksen kohdistuessa tiettyyn ajalliseen ja paikalliseen tapahtumaan, puhutaan **tilanneymmärryksestä**. Tilanneymmärrystä harvoin täysin saavutetaan.

Päättely (kuvio 1) tarkoittaa hermeneuttista ja kognitiivista prosessia, jossa tietämyksen perusteella edetään perusteltuun johtopäätökseen ajattelun, puolueettoman tarkastelun ja oivaltamisen avulla.

Viisaus (engl. wisdom, sapience) (kuvio 1) tarkoittaa kykyä käyttää dataa, informaatiota ja tietämystä oikealla tavalla eli keskittyä oikeisiin asioihin (priorisointi) ja tehdä oikeita päätöksiä päättelyyn pohjautuen. Viisauteen sisältyy moraaliset ja eettiset periaatteet, joiden perusteella erotellaan hyvät ja huonot päätökset toisistaan (Cooper 2017, 55). Tiettyyn ajalliseen ja paikalliseen tapahtumaan liittyvästä johtopäätöksestä käytetään nimitystä **tilannevaste** (engl. situational response). Viisaus osana tilannevastetta ei ole itsestäänselvyys ja sen poissaolo voi näkyä esimerkiksi organisaatioissa päätöksinä, joissa riskit kasvavat tai tehottomuus lisääntyy. Toisaalta viisaat ja oikeat tilannevasteet parantavat organisaation resilienssiä tulevien muutosvoimien varalle. (Pettit ym. 2010, 8) Tätä ilmiötä käsitellään tarkemmin luvussa 7.2.

4 TEOREETTINEN VIITEKEHYS

Tässä luvussa raportoidaan tutkimuksen sijoittuminen osana yleistä tutkimuskenttää, teoreettiset näkökulmavalinnat ja teorian yhdistyminen empiriaan. Luvun tarkoituksena on selvittää aiheesta tehty aiempi tutkimus. Lopuksi esitellään uusi yhdistelty ja sovellettu teoreettinen viitekehys, jonka avulla voidaan jäsentää, mallintaa ja hahmotella kybertilannekeskusten vaikutuksia organisaation kyberresilienssiin.

4.1 Rakenneanalyyttinen paradigma

Ennen toista maailmansotaa organisaatioiden ajateltiin olevan suljettuja järjestelmiä, joiden toiminnassa ei tarvitse ottaa ympäristöä huomioon (Seeck 2008, 160). Samalla ajateltiin, että tieteellisellä tutkimuksella kyettäisiin löytämään kaikille organisaatioille ainoita oikeita tapoja järjestää toimintaansa (Seeck 2008, 193). Edellä kuvattu tieteellisen liikkeenjohdon ja ihmissuhdekoulukunnan paradigmojen näkökulma organisaation toimintaa ei riittänyt 1950-luvulla kohdattuihin uusiin organisaatioiden haasteisiin: tietojenkäsittelyn kehittyminen, organisaatioiden koon kasvamisen johtaminen byrokratisoitumiseen sekä kansainvälistymisen ja globalisaation myötä entistä monimutkaisemmat ulkoistusrakenteet (Guillén 1994, 12-13).

Toisen maailmansodan päättyminen, siitä juontuva teknologinen kehittyminen ja armeijan keskeinen rooli tuottivat uusia ideoita sekä painetta organisaatioiden johtamisen ja toiminnan muutoksiin (Seeck 2008, 161). Näiden vielä nykyäänkin ajankohtaisten ongelmien johdosta syntyi uusi rationaalinen taloudelliseen nousukauteen ajoittuva rakenneanalyyttinen paradigma, joka pystyi vastaamaan näihin haasteisiin (Barley & Kunda 1992, 189-193).

Rationaalisella paradigmalla tarkoitetaan ideologisia ja teknisiä tapoja ajatella organisaatio ”koneeksi” ja sen ”osiksi” – mekaaniseksi tai tietojenkäsittelylliseksi. Organisaation toimintaa muuttamalla tai manipuloimalla erilaisilla metodeilla voidaan lisätä kokonaisuuden tehokkuutta. Henkilöstö nähdään rationaalisessa paradigmassa asiantuntijoiksi, jotka toimivat laskelmoidusti kokemuksensa perusteella organisaation hyväksi ja pitävät tärkeänä hyvin suunniteltua ja taloudellisesti tehokasta järjestelmää. Rationaalisen paradigman vastinpari on normatiivinen paradigma, jossa organisaatio nähdään yhteisönä, vapaa-aikaa tai

työtä ei erotella ja esimiehet johtavat esimerkillään työntekijöiden kanssa samalla tasolla. (Barley & Kunda 1992, 384; Seeck 2008, 38)

Rakenneanalyyttinen paradigma on edellä kuvatulla tavalla rationaalinen paradigma, jossa organisaatio ajatellaan ympäristöstään riippuvaisena ja sen vaikutuksessa jatkuvasti olevana avoimena järjestelmänä (Seeck 2008, 161). Tämä tarkoittaa organisaation ympärillä olevien tekijöiden jatkuvaa huomioimista osana omaa toimintaa sekä organisaatiorakenteen valitsemista ja jatkuvaa mukautumista kontingentisti eli tilannesidonnaisesti (Clegg & Hardy 1999, 57).

Ongelmia pyritään ratkaisemaan vertailemalla erilaisia käytänteitä, organisaatiorakennemalleja ja päätöksentekoon liittyviä malleja. Rakenneanalyyttinen paradigma muodostaa tämän tutkimuksen teoreettisen asemoitumisen pohjan, sillä se mallintaa hyvin kybermaailmassa toimivien organisaatioiden avointa rakennetta, liittyy vahvasti tietojenkäsittelyn kehittymiseen ja selittää globaalien kybermaailmassa toimivien organisaatioiden haasteita keskinäisen kytkeytymisen ja digitaalisten rakenteiden kautta. Rakenneanalyyttiseen paradigmaan kuuluvat muun muassa tässä tutkimuksessa käytettävät järjestelmäteoria ja sen ilmentymä kybernetiikka sekä laaja joukko muita tämän tutkimuksen ulkopuolelle jätettyjä teoreettisia näkökulmia. (Guillén 1994; Seeck 2008, 162-163)

Tämän tutkimuksen ulkopuolelle jää rajaussyistä monia lähiteorioita ja malleja, joista voisi olla hyötyä kybertilannetietoisuuden ja kyberresilienssin tutkimuksessa. Esimerkkinä edellisistä informaatioteoria (engl. information theory) ja soveltavien tieteiden joukosta matemaattiset operaatioanalyysi ja katastrofiteoria. Lisäksi kompleksisuusteoreettiset mallit, kuten kompleksisten adaptiivisten järjestelmien hyödyntäminen olisi voinut tuoda hieman erilaisen näkökulman resilienssimallin laadintaan. Kompleksisten adaptiivisten järjestelmien monitieteisessä mallissa keskitytään lähinnä järjestelmien korkean tason ominaisuuksiin. Mallissa sosiaaliset monimutkaiset vuorovaikuttavat verkostot muodostavat kokonaisuuden, jota ei voida ymmärtää osiensa kautta. (Miller & Page 2009, 3, 40-41, 44-45 ja 93)

4.2 Järjestelmäteoria

Järjestelmä tai systeemi (engl. system) juontuu 1600-luvulta kreikankielisten sanojen *syn-* eli ”yhdessä” ja *histanai* eli ”aiheuttaa” yhdistelmästä *synistanai* eli ”sijoittaa yhteen, järjestellä

tai muotoilla". Myöhemmin sana muuttui muotoon *systema*, joka tarkoitti organisoitua kokonaisuutta, joka rakentuu osista. (Harper 2019; Merriam-Webster 2019b) Systeemi-sanan etymologia kuvaa hyvin myös järjestelmäteorian (engl. System Theory) sisältöä, jossa tutkitaan kokonaisvaltaisesti ja tiederajat ylittävästi järjestelmiä eli osista muodostuvia systeemejä (von Bertalanffy 1968, 54).

Tässä tutkimuksessa järjestelmäteorialla viitataan yleiseen järjestelmäteoriaan (engl. General System Theory, GST), jonka itävaltalainen biologi Ludwiq von Bertalanffy kehitti kahdessa vaiheessa 1930 ja 1940-luvuilla. Yleisen järjestelmäteorian käsitteet ovat toimineet historiallisesti pohjana organisaatioiden tarkastelussa järjestelmänäkökulmasta. (Seeck 2008, 162)

Järjestelmäteorian syntyyn vaikuttaneita tekijöitä on ollut useita. Ensimmäiseksi, on ollut tarve monien tieteiden väliselle yhtenäiselle ja yleiselle ilmiöiden tarkasteluun tarkoitetulle teoreettiselle mallille. Tämä sopii hyvin kyberresilienssin tutkimukseen, jossa yhdistyy monen tieteenalojen teoreettinen tausta. (von Bertalanffy 1968, 91-94)

Toiseksi, eri tieteenaloilta on löydetty järjestelmille yhteneväisiä piirteitä, joille ei aikaisemmin ollut yhteistä luokittelua. Nämä piirteet kuvaavat hyvin kyberympäristössä toimivien organisaatioiden ja järjestelmien olemusta ja käyttäytymistä. (von Bertalanffy 1968, 91-94)

Kolmanneksi, uuden tieteellisesti kehittyvän ilmiön - organisoidun kompleksisuuden - haasteisiin ja tutkimiseen tarvittiin uusia työkaluja. Kyberympäristö on ihmisen luoma jatkuvasti kasvava kompleksinen kokonaisuus, jonka ymmärtämiseen järjestelmäteorialla on paikkansa. (von Bertalanffy 1968, 91-94)

Neljänneksi, yhteen tieteenalaan sidottuja käsitteitä on pyritty saamaan laajempaan käyttöön tiederajat ylittävästi kuvaamaan ilmiöitä kaikissa järjestelmissä. Tämä sopii hyvin kybertilannekeskusten ja resilienssin tutkimiseen, jossa yhdistyvät ihmisten, teknologian ja organisaatiotutkimuksen elementit. (von Bertalanffy 1968, 91-94)

Kaikissa edellä mainituissa neljässä järjestelmäteorian tavoitteessa korostuvat tieteidenvälisyys, siiloutumisen karsiminen ja kokonaisvaltainen lähestymistapa järjestelmiin ja tieteeseen ylipäätään.

4.2.1 Kyberavaruuden organisaation ominaisuudet järjestelmänä

Järjestelmäteoreettisesta näkökulmasta ”**järjestelmä**” tarkoittaa luonnon tai ihmisen muodostamaa vuorovaikuttavien osien kokonaisuutta (von Bertalanffy 1968, 4). Järjestelmiä esiintyy monilla tieteenaloilla ja monissa kokoluokissa. Esimerkkeinä tilannehuone, sarana, tietokone, munasolu, huonekasvi, koira, työntekijä, kybertilannekeskus, ohjelmointikielet ja aurinkokunta (mukaellen Boulding 1956; von Bertalanffy 1968, 28-29). Näillä kaikilla järjestelmillä on yhteneväisiä toimintaa ohjaavia ominaisuuksia ja periaatteita tieteenalasta riippumatta. Nämä ominaisuudet ja periaatteet esitetään seuraavissa alaluvuissa, joissa käsitellään järjestelmäteorian keskeisiä elementtejä (kuvio 2).

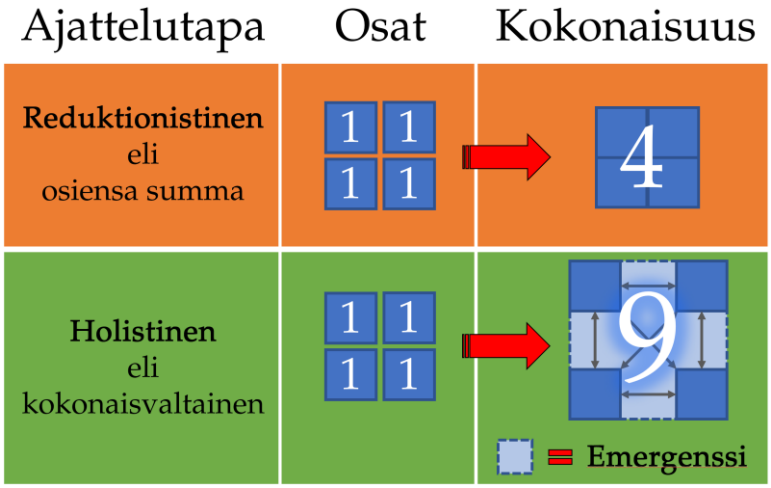
Kuvio 2. Järjestelmäteorian mukaisia järjestelmän ominaisuuksia. (Boulding 1956)

4.2.1.1 Kokonaisvaltaisuus eli holismi

Satoja vuosia ennen ajanlaskun alkua Aristoteles esitti ajatuksensa eroavaisuuksista ja yhteneväisyyksistä metafysiikkaa käsittelevän kirjasarjansa kahdeksannessa ”Eta”-kirjassa: ”*kokonaisuuden osat muodostavat yhdessä enemmän, kuin niiden yhteenlaskettu määrä*” (Aristoteles, 300 e.a.a.; Phelan 1999, 237). Puolestaan vuonna 1926 eteläafrikkalainen pääministeri Jan Christian Smuts tiivisti Aristoteleen ajatuksen muotoon ”*kokonaisuus on enemmän, kuin osiensa summa*” (Smuts 1926, 101). Smuts kehitti tälle tieteenfilosofiselle ajattelutavalle nimen **holismi** (Smuts 1926, V). Kokonaisvaltaisuuden merkitystä korostavaa holismia Smuts tarkasteli biologisen organismin avulla. Organismi koostuu osista ja muodostaa yhtenäisenä kokonaisuuden, joka on enemmän, kuin organismin osat yhteen laskettuna. Organismin osat ovatkin jatkuvassa yhteydessä ulkoisesti ja sisäisesti muodostaen kompleksisen koko-

naisuuden. Jos organismi hajotetaan palasiksi, ei sitä pystytä enää kasaamaan takaisin entisenlaiseksi kokonaisuudeksi, sillä kokonaisuus muodostuu organismin osien sisäisistä toiminnoista, riippuvuuksista ja suhteista. (Smuts 1926, 101-103)

Holismin vastakohta on reduktionistinen ajattelutapa, jossa kokonaisuudet koostuvat osista, joilla on vain vähän tai ei ollenkaan keskinäistä avointa vuorovaikutusta keskenään. Reduktionistisesti ajateltuna systeemi ei ole enempää tai vähempää, kuin osiensa täsmällisesti määritelty summa. (von Bertalanffy 1968, 19)



Kuvio 3. Reduktionistisen eli osien summasta koostuvan ja holistisen eli kokonaisvaltaisen näkökulman eroavaisuudet ja yhteneväisyydet.

Järjestelmäteorian mukaan edellä kuvattu perinteinen reduktionistinen järjestelmien osien muodostaman kokonaisuuden tulkinta ei päde järjestelmissä, jotka ovat jatkuvasti avoimessa vuorovaikutuksessa sisäisesti ja ulkoisesti (von Bertalanffy 1968, 18). Sisäiset vuorovaikutussuhteet, järjestelmän luonne ja toiminnot muodostavat järjestelmään ”enemmän”, kuin osat erikseen yhteenlaskettuna (Smuts 1926, 102). Tässä kontekstissa ”enemmän” ei välttämättä tarkoita järjestelmän hyödyllisyyttä tai haitallisuutta, vaan osien keskinäisestä vuorovaikutuksesta muodostuvia uusia ylemmällä tasolla olevia ominaisuuksia tai ilmiöitä eli **emergenssejä**. Tällaiset ominaisuudet voivat aiheuttaa järjestelmään joko hyötyä tai haittaa. Keskeistä on, että järjestelmien emergentit ominaisuudet eivät ole palautettavissa järjestelmien erillisten osien yksittäisiksi ominaisuuksiksi, vaan ne ovat kokonaisvaltaisen toiminnan tulosta (kuvio 3). (Tieteen termipankki 2019l)

Toisaalta järjestelmän muodostamien osien ominaisuuksien yhteisvaikutus voi olla sattumalta myös sama, kuin reduktionistisesti – eli erillisinä – ajateltujen osien yhteenlaskettu vaikutus. Tästä huolimatta holistinen eli kokonaisvaltainen ajattelutapa pitää sisällään enemmän, kuin reduktionistinen ajattelutapa – kuten järjestelmän sisäiset vuorovaikutussuhteet, kokonaisvaltaisen luonteen ja yhteisvaikutuksen. Holistisessa mallissa järjestelmässä vallitseekin osien keskinäisriippuvuus: muutos yhteen järjestelmän osaan vaikuttaa

koko järjestelmän tilaan riippuen muiden vaikutetuksi tulleiden elementtien toiminnasta (von Bertalanffy 1968, 66). Järjestelmäteoriassa tällaisia vahvojen sisäisten vuorovaikutussuhteiden järjestelmiä kutsutaan myös organisoiduiksi kokonaisuuksiksi tai organisoiduiksi kompleksisuuksiksi (von Bertalanffy 1968, 19 ja 37). Matemaattisesti ajateltuna osat muodostavat kokonaisuuden 1+1+1+1+x = 4+x = 9, jossa x = kokonaisuuden aikaansaama emergenssi eli x = 5.

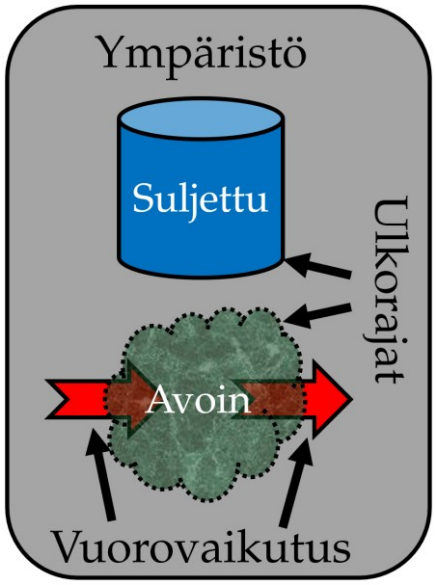
Kyberturvallisuuden näkökulmasta holistisuus vaatii kokonaisvaltaisen ajattelutavan organisaation kyberresilienssin parantamiseksi. Käytännössä kybertilannekeskustoiminnassa tulee ottaa huomioon mahdollisimman laajasti kaikki kyberavaruuden muutosvoimat. Pieneltäkin tuntuvalla uhalla voi olla lopputuloksen kannalta ratkaiseva merkitys. Samalla tulee ymmärtää, että organisaation turvallisuus on kokonaisuus ja muodostuu huomattavasti kybertilannekeskustoimintaa laajemmasta toiminnasta. Kybertilannekeskuksella ei voida yksinään parantaa koko organisaation resilienssiä. Esimerkiksi varautuminen pitää sisällään huomattava määrän jatkuvuussuunnitteluun liittyviä näkökohtia, jotka vaikuttavat kyberresilienssiin. Esimerkiksi organisaation johdon sitoutuminen, turvallisuustoiminnan suunnittelu ja ohjaus, päätöksentekoprosessit, järjestelmien ylläpito, henkilökunnan toiminta ja asenteet. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 23-26 ja 37-39)

Kokonaisvaltaisuus korostaa yhteistyön merkitystä kyberresilienssin parantamiseksi. Toimivalla ja tiiviillä vuorovaikutuksella eli yhteistyöllä suojattavan organisaation kanssa on mahdollista saavuttaa emergenssin avulla positiivista **synergiaa** (kreik. syn = yhdessä, ergon = työ) eli yhteisvaikutusta (Read 1999, 1273; Tieteen termipankki 2019c). Sama pätee kybertilannekeskustoimialan verkostoyhteistyöhön. Tilanteessa, jossa kyberavaruuden turvallisuutta ei suojattaisi yhteistyössä, on mahdollista syntyä tilanne **antagonismille**, jossa kyberresilienssiä parantamaan tarkoitetuilla toimenpiteillä onkin vastakkaiset vaikutukset ja yhteisvaikutus on huonompi, kuin erillisten toimenpiteiden vaikutus yksinään (Tieteen termipankki 2019p). Kybertilannekeskuksen tulee olla aktiivisessa yhteydessä suojattaviin organisaatioihin ja varmistaa erilaisin sopimuksin, että kyberresilienssiin vaikuttavat osa-alueet ovat hallinnassa kokonaisvaltaisesti. Verkostokumppanien kanssa tehtävällä yhteistyöllä voidaan saavuttaa laajempia synergiaetuja esimerkiksi kyberuhka- ja haavoittuvuustiedonvaihdon osalta.

4.2.1.2 Rajautuvuus ja itsesäätely

Kaikilla järjestelmillä on ulkorajat, jotka voidaan tunnistaa vuorovaikutussuhteiden voimakkuuserojen perusteella. Rajojen määrittely mahdollistaa järjestelmän erottamisen muista järjestelmistä, tutkimisen ja nimeämisen. Kaikkien järjestelmien rajat ovat dynaamisia eli muuttuvia. Järjestelmät voidaan jakaa rajojensa toimintaperiaatteen mukaisesti **avoimiin** ja **suljettuihin** järjestelmiin. Avoin järjestelmä on jatkuvassa vuorovaikutussuhteessa ympäristönsä kanssa. Avoimen järjestelmän rajat ovat luonteeltaan dynaamisia, eli niitä ei voida välttämättä määritellä tarkasti, mutta ne ovat olemassa. Suljetulla järjestelmällä ei ole mitään vuorovaikutussuhteita ympäristönsä kanssa. Esimerkiksi kaikki elävät organismit ovat avoimia järjestelmiä. Suljettuja järjestelmiä käsitellään tyypillisesti teoreettisesti, eikä niitä todellisuudessa juurikaan esiinny. (von Bertalanffy 1968, 19,39,141 ja 215)

Järjestelmäteoriassa kaikki järjestelmät ovat avoimia. Kuviossa 4 on esitetty suljetun ja avoimen järjestelmän toimintaerot samassa ympäristössä. Avoin järjestelmä vaihtaa ainetta, energiaa ja dataa ympäristönsä kanssa. Se ottaa sitä dynaamisesti muuttuvien rajojensa sisäpuolelle sekä siirtää sitä rajojensa ulkopuolelle. Suljettu järjestelmä toimii täysin eristetysti, eikä sen rajojen läpi ole pääsyä. (von Bertalanffy 1968, 141,149,159 ja 163)



Kuvio 4. Havainnollistus avoimen ja suljetun järjestelmän eroista. Molemmilla on ulkorajat, mutta avoin järjestelmä päästää rajojen lävitse vuorovaikutusta.

Kyberturvallisuuden ylläpidon näkökulmasta avoimen järjestelmän toimintaperiaate korostaa tilanteenmukaista toimintaa ja hylkää mahdollisuuden eristäytyä. Nykyorganisaatioilla esimerkiksi verkkoyhteydet ulkoiseen kyberavaruuteen ovat olemassaolon edellytys. Tämä mahdollistaa haitallisen datan kulkeutumisen organisaation tietotekniseen kyberavaruuteen. Tällöin korostuu avoimen järjestelmän rajoilla ja sisäpuolella tilannetietoisuuden merkitys ja ennakoivat varautumistoimenpiteet uhkien toteutuessa. Esimerkiksi yhden kyberuhilta suojaavan ulkokuoren sijasta tulisi olla käytössä kerroksellisia, eristäviä ja toiminnan jatkuvuuden säilyttäviä hallintakeinoja eli kyvykkyyksiä, joilla rajoista läpipäässeet uhat voidaan tehdä vaarattomaksi, torjua paikallisesti tai leviäminen estää. Näin toimii esimerkiksi ihmisen puolustus- eli immuunijärjestelmän vasta-aineet ja

imusolut taudinaiheuttajia ja viruksia vastaan (Mustajoki 2018). Kyberturvallisuutta kehittävä ajattelutapa onkin, että haitalliset toiminnot ovat jo päässee rajojen sisäpuolelle, mutta niitä ei olla huomattu. Tämä korostaa tilannetietoisuuden ja varautumisen merkitystä osana organisaation kyberresilienssin hallintaa.

4.2.1.3 Tavoitehakuisuus

Järjestelmäteorian mukaan kaikki järjestelmät ovat tavoitehakuisia. Tavoitteellisuus voidaan jakaa teleologisesti eli päämääriltään kahteen luokkaan: (1) staattisiin ja (2) dynaamisiin. Staattinen tavoite tarkoittaa päätösten sopivuutta tiettyyn muuttumattomaan tarkoitukseen. Dynaaminen tavoite puolestaan kuvaa, miten suoraviivaisella prosessilla määriteltyyn tavoitteeseen päästään. Dynaamiseen tavoitteeseen pääsemisen prosessia voidaan tarkastella kolmesta näkökulmasta:

1. rakenteiden järjestely johdattaa järjestelmän toimintaa kohti tavoitetta (palaute),
2. samaan tavoitteeseen päästään eri lähtökohdista eri menetelmin (ekvifinaliteetti) ja
3. käyttäytyminen määrittyy tavoitteen ennustamisen perusteella (suunnitelma).

(Harisalo 2008, 181; von Bertalanffy 1968, 75-79)

Kyberavaruus ja organisaatiot avoimina järjestelminä ovat jatkuvasti muutoksessa (dynaaminen). Tällöin nykytilanteen mukaan tehty päätös (staattinen) on hetken kuluttua vanhentunut, eikä välttämättä johda alun perin tavoiteltuun lopputulokseen. Samojen staattisten ratkaisujen toistaminen ympäristön muutoksista huolimatta ei siten ole vaihtoehto kyberresilienssin ylläpitämiseksi tai parantamiseksi. Tavoitteisiin pääseminen vaatii jatkuvia korjausliikkeitä ja toimintatapojen muokkaamista. Korjaavat toimenpiteet tehdään kyberavaruuden tilannetietoisuuteen pohjautuvan palautteen avulla.

Ekvifinaliteetti eli samatavoitteisuus tarkoittaa kyberturvallisuusnäkökulmasta esimerkiksi sitä, että korkean kyberresilienssin saavuttamiseksi ei ole yhtä ainoaa oikeaa tapaa (Ihanus & Pakarinen 2010). Järjestelmällä onkin vapausasteita eli mahdollisuus saavuttaa sama tavoite eri keinoin. Hyvään kyberresilienssiin voidaan päästä monista lähtökohdista monin oikeansuuntaisin keinoin – suoremmin tai epäsuoremmin. Tavoitteeseen mahdollisimman suoraan pääsemisessä auttaa selkeä suunnitelma ja näkemys vaadituista vaiheista ja toimenpiteistä. Suunnitelmaa tulee päivittää jatkuvasti ympäristön tilan muutosten mukaisesti

eli tilannetietoisesti, jotta tavoitteet saavutetaan mahdollisimman suoraviivaisesti. (von Bertalanffy 1968, 79)

Kyberavaruudessa toimiva organisaatio parantaa kyberresilienssiä parhaiten, kun sillä on selkeä tavoite, ymmärrys nykytilasta, omaan tarkoitukseen räätälöidyt keinot ja suunnitelma tavoitteeseen pääsemiseksi.

4.2.1.4 Eriytyminen eli segregaatio

Kokonaisvaltaisessa järjestelmässä tapahtuvaa osasten eli elementtien eriytymistä tai irtaantumista toisistaan kutsutaan segregaatioksi. Eriytyminen tarkoittaa lisääntyvää itsenäisyyden astetta, jota kutsutaan itseorganisoitumiseksi. Kaikissa kokonaisvaltaisissa järjestelmissä tapahtuu järjestelmäteorian mukaan kilpailua, jota voidaan kuvata järjestelmän elementtien väliseksi ”kinasteluksi”. Kilpaileminen liittyy vahvasti kasvuun, sillä kilpaileminen johtaa ajan kuluessa pienintä kasvua saavuttavan järjestelmän tuhoutumiseen ja muiden selviämiseen. Kasvu voi olla ajallista tai suhteellista muihin järjestelmiin nähden. Kasvu on mahdollista jatkuvan segregaation, rajautuvuuden ja tavoitehakuisuuden avulla, jossa järjestelmän osaset kasvavat erilleen toisista järjestelmistä. (von Bertalanffy 1968, 63-68 ja 96-97)

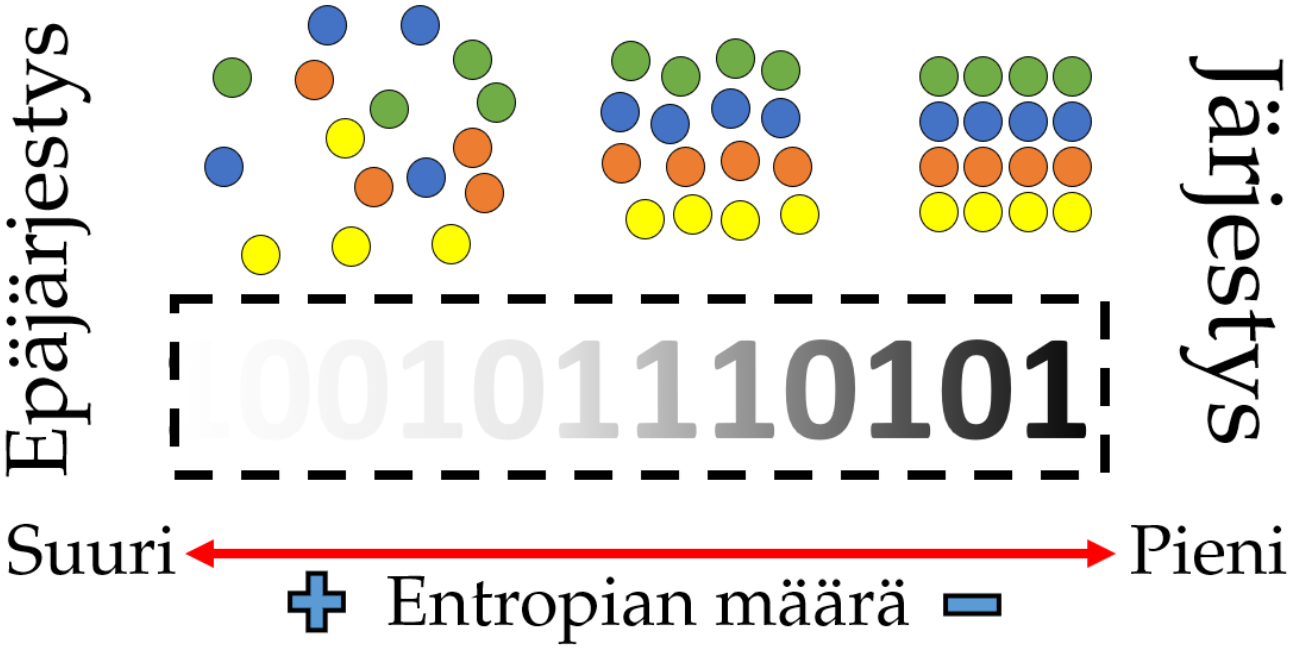
Kyberavaruudessa toimiva organisaatio joutuu kilpailemaan monenlaisia kyberuhkia vastaan, jossa kyberturvallisuutta uhkaavilla muutosvoimilla on tyypillisesti etulyöntiasema. Esimerkiksi pahamieliset kyberrikolliset voivat suunnitella iskuaan pitkään ennen varsinaista toimintaa, johon kyberavaruudessa toimivan kohdeorganisaation tulee olla varautunut kehittämällä kyvykkyyksiä ja kyberresilienssiään. Tällöin kilpailun voidaan ajatella perustuvan kyvykkyyksiin ja niiden parantamiseen. (von Bertalanffy 1968, 63-68)

Kyberavaruudessa kilpaillaan paitsi haitallisia voimia vastaan, myös muiden kyberavaruuden toimijoiden kanssa. Tällöin yhteiset toimintatavat ja verkostot mahdollistavat kybertoiminnan ylipäänsä. Eriytyminen ei siis tarkoita, etteikö eriytyneillä järjestelemillä olisi keskinäistä vuorovaikutusta. Esimerkiksi yhteistyöverkostot, toimintastandardit ja tietojen vaihtaminen palvelee kaikkia lain mukaan oikein toimivia kyberavaruuden toimijoita. Lisäksi kyberavaruuden luonteesta johtuva tekninen keskinäisriippuvuus pakottaa järjestel-

mät tekemään yhteistyötä ja sopimaan yhteisistä toimintamalleista. Esimerkiksi kybertilannekeskusten keskinäinen tietojenvaihto parantaa kaikkien osapuolten tilannetietoisuutta vastavuoroisuusperiaatteella.

4.2.1.5 Hierarkkisuus ja entropia

Entropia eli haje on järjestelmän epäjärjestyksen mitta. Mitä enemmän järjestelmässä on entropiaa, sitä vähemmän on järjestystä eli hierarkiaa. (Tieteen termipankki 2019q) (kuvio 5) Termodynamiikan toisen lain mukaisesti suljetuissa järjestelmissä entropia eli epäjärjestys kasvaa jatkuvasti ajan kuluessa. Sen sijaan avoimissa järjestelmissä entropia voi olla positiivista, negatiivista tai neutraalia eli epäjärjestys voi kasvaa, vähentyä tai pysyä samana. Perussääntö on, että kaikissa peruuttamattomissa prosesseissa epäjärjestys kasvaa ajan kuluessa. Toisin sanoen järjestelmä luhistuu, kutistuu ja rakenteet katoavat ilman jatkuvaa ylläpitoa. Lopulta järjestelmä kuolee eli tuhoutuu. (Groot & Mazur 1984, 20-22; von Bertalanffy



Kuvio 5. Entropian eli hajeen ja järjestyksen suhde esitettynä graafisesti. Kuviossa vasemmalla epäjärjestys kasvaa ja oikealla järjestys on suurinta.

Hierarkkisuus viittaa järjestelmäteorian näkemykseen, jonka mukaan kaikki järjestelmät ovat luokiteltavissa ja koostuvat elementeistä, joilla on rakenteita ja prosesseja. Elementtien välillä on järjestystä eli hierarkiaa. Esimerkiksi evoluutio on tuottanut ajan saatossa hierarkiaa biologisten järjestelmien välille (Montévil & Mossio 2015, 179). Vastaavasti hierarkian avulla voidaan kuvata esimerkiksi tilannetietoisuuden muodostumisen prosessi. Luvussa

4.2.2 on esitetty tarkempi analyysi hierarkian yhteydestä tilannetietoisuuden muodostumiseen.

Negatiivinen entropia tarkoittaa, että avoin järjestelmä voi lisätä tai pitää nykyisen organisoitumisen asteensa. Näin huolimatta siitä, että ympäristössä vallitsee hajaannus, sekasotku ja kaaos. Tämä näkyy järjestelmässä esimerkiksi toimintatapojen kehittymisenä, rakenteiden muuttumisena ja resurssien lisääntymisenä. Järjestelmäteorian mukaan hierarkkista järjestystä on kaikissa maailmankaikkeuden rakenteissa (osien järjestyksessä) ja toiminnoissa (prosessien järjestyksessä). (von Bertalanffy 1968, 26-27)

Data on ilmentymä negatiivisesta entropiasta ja sen avulla voidaan mitata järjestäytyneisyyden astetta. Mitä enemmän järjestelmässä on dataa, sitä vähemmän on entropiaa eli epäjärjestystä. Organisoitumisen lisääminen ja ylläpito edellyttävät vuorovaikutusta datan saamiseksi ympäristöstä. (von Bertalanffy 1968, 42, 125 ja 150)

Kyberturvallisuuden näkökulmasta kyberavaruudessa toimivan organisaation on jatkuvasti resursoitava kyberresilienssin ylläpitoa. Ilman resursseja eli energiaa ylläpito vähenee, joka vaikuttaa kyberresilienssiin heikentävästi. Kybertilannekeskuspalvelun tuottaminen tarvitsee riittävät resurssit, jotta kohdeorganisaation kyberresilienssiä voidaan ylläpitää tasapainoisesti. Resurssien lisäksi on oltava kyky tuottaa riittävästi dataa tilannetietoisuuden muodostumiseen kyberavaruudesta – organisoidun kompleksisuuden ympäristöstä.

4.2.1.6 Mukautuvuus ja resilienssi

Järjestelmäteorian mukaan järjestelmät pyrkivät mukautumaan ympäristön muutoksiin ja hakeutumaan tasapainoiseen tai vakaaseen tilaan (engl. steady state), jonka saavuttamisen ympäristön muutos tekee lopullisesti mahdottomaksi. Tästä voidaan pitää todisteena fysikaalisista, kemiallisista ja sosiaalisista järjestelmistä muodostunutta nykymaailma, jota ilman tätä periaatetta ei voisi olla olemassa. Täydellisen maailman tasapainon ja jähmettymisen sijaan hallitut muutosvoimat mahdollistavat maailman kehittymisen ajan ja muiden järjestelmin suhteen. (von Bertalanffy 1968, 158 ja 203) Tämä tarkoittaa, että muutos on hallittuna mahdollisuus ja hallitsemattomana mahdollinen uhka.

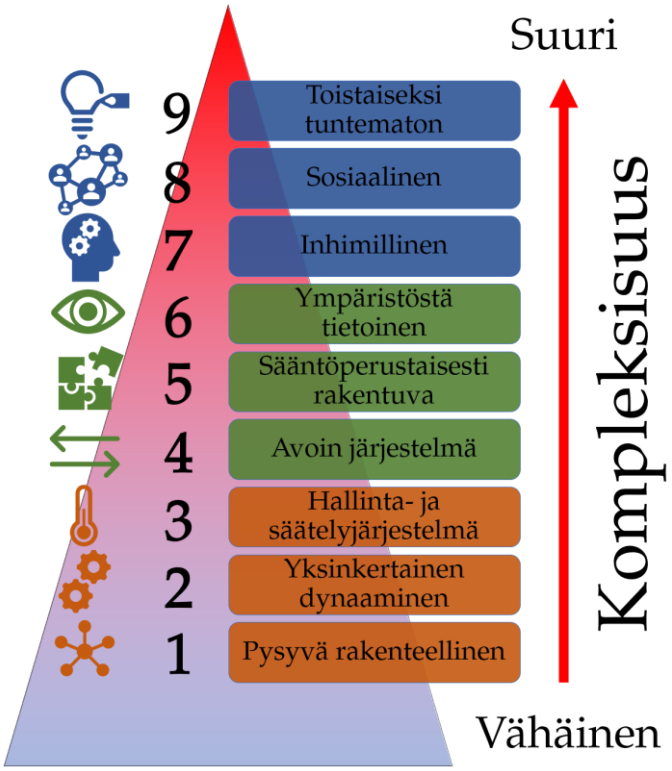
Vakaan tilan tavoittelu on jokaisen järjestelmän tavoitteena, sillä toiminnan edellytykset ovat silloin optimaalisimpia. Tämä pätee myös kyberresilienssiin. Tasapainoisessa kyber-

resilienssissä kyvykkyydet ja haavoittuvuudet ovat tasapainossa. Jos kyvykkyydet tai haavoittuvuudet korostuvat toisiinsa nähden liikaa, ei toiminta ole optimaalista. Tällöin organisaatio menettää etuaan suhteessa muihin ja ajan myötä tuhoutuu. (Pettit ym. 2010, 6-7; Taskinen 2018, 18)

Kyberturvallisuuden näkökulmasta kybertilannekeskus on paikka, joka koordinoi kyvykkyyksien eli hallintakeinojen määrää ja seuraa tilannetietoisesti muutosvoimien aiheuttamia haavoittuvuuksia. Kybertilannekeskuksen tehtävä on ylläpitää tasapainoista kyberresilienssiä, jolla varmistetaan kyberavaruudessa toimivan organisaation toiminnan jatkuvuus ja toipuminen haitallisista kybertapahtumista huolimatta. Muuttuvasta kyberavaruudesta johtuen kyvykkyyksien ja muutosvoimien tasapainoa on jatkuvasti ohjattava optimaalisen toiminnan takaamiseksi.

Tasapainoa tavoittelevaa ympäristön muutoksiin mukautuvaa prosessia voidaan mallintaa järjestelmäteorian johdannaistieteen kybernetiikan avulla, jota hyödynnetään tässä kontekstissa luvussa 4.2.3.

4.2.2 Järjestelmien kompleksisuuden ja tilannetietoisuuden suhde



Kuvio 6. Järjestelmien kompleksisuusluokat numeroituna ja luokiteltuna eri värein. Kuviossa kompleksisuus on vähäisintä alareunassa ja suurinta yläreunassa. Symbolit linkittyvät seuraavien alalukujen mukaisesti.

Järjestelmäteorian keskeinen osa on järjestelmien kompleksisuuden tutkiminen. Kompleksisuutta tutkitaan erityisesti kompleksisuusteoreettisissa järjestelmäteorian johdannaistieteissä. (Phelan 1999, 237-238) Kenneth Boulding julkaisi vuonna 1956 artikkelin, jossa järjestelmäteoriaa jatkojalostetaan muodostamalla teoreettisille järjestelmille hierarkia eli järjestys niiden kompleksisuuden mukaan. Kompleksisuuden käsite on määritelty jo aiemmin luvussa 3.2.1.

Bouldingin kokonaisvaltaisessa ja poikkitieteellisessä mallissa jokainen teoreettinen kompleksisuuden taso vastaa eli

kategorisoi empiirisessä todellisuudessa monia järjestelmiä. Toisin sanoen malli kuvaa reaalimaailmasta löytyvien järjestelmien kompleksisuutta jakaen järjestelmät yhdeksään kompleksisuusluokkaan (kuvio 6). (Boulding 1956, 202)

Bouldingin kehittämää systeemien kompleksisuuden hierarkiaa on tutkittu ja sovellettu muun muassa organisationaalisen oppimisen (Nair 2001), digitalisaation (Tokody 2018) ja verkkopohjaisten sovellusten tutkimuksessa (Bartuskova & Krejcar 2014). Mallia on myös kritisoitu yleistävyydestään. Esimerkiksi Mingers kysyy, minkä tarkkojen tekijöiden mukaan järjestelmiä voidaan jaotella eri kompleksisuustasoihin: elementtien määrän, järjestelmien ulkopuolisten yhteyksien määrän vai toimintojen erilaistumisen mukaan? Tämän seurauksena mallia on pyritty jatkokehittelemään (Mingers 1997, 306-307).

Tässä tutkimuksessa Bouldingin järjestelmien kompleksisuuden hierarkiamallin ja edellä käsiteltyjen muiden artikkeleiden pohjalta on muodostettu kybertilannekeskuksen kontekstia kuvaava lähestymistapa. Lähestymistavan rakenne on kuvattu kuviossa 6. Mallin tasot on nimetty eri tavalla, kuin Bouldingin alkuperäisessä artikkelissa, mutta sisältö noudattelee alkuperäisen mallin ideaa. Pyramidin alaosassa ovat järjestelmät, joiden ominaisuutena kompleksisuus on vähäistä. Siirryttäessä oransseista alemmista kompleksisuustasoista kohti sinisellä värillä merkittyä pyramidin kärkeä järjestelmät sisältävät kumuloituvasti alemman tason järjestelmien ominaisuudet, jolloin kompleksisuuden määrä nousee.

Kukin taso on jaettu tässä tutkimuksessa värikoodauksella kolmeen luokkaan tilannetietoisuuden suhteen: nykytilanne (tasot 1-3, oranssi), kehityssuunta (tasot 4-6, vihreä) ja kokoavat tasot (tasot 7-9, sininen).

Nykytilanne viittaa järjestelmien kytkeytyneisyyden ja kompleksisuuden määrään tällä hetkellä kybertoiminnassa. Kehityssuunta tarkoittaa suuren kiinnostuksen ja kehityksen alla olevia kompleksisuustasoja, joiden kehittymistä odotetaan lähitulevaisuudessa teknologisesta ja tutkimuksellisesta näkökulmasta. Kokoavat tasot liittyvät kompleksisuustasoihin, joiden sisältämien järjestelmien voidaan ajatella toistaiseksi luovan lopullisen tilannetietoisuuden ja -ymmärryksen. Kokoavien tasojen perimmäinen ymmärtäminen antaa mahdollisuuden ihmisten ja organisaatioiden tilannetietoisuuden ja resilienssin kehittämiseen. Tällainen ajattelutapa on peräisin emergentin materialismin ontologisesta tieteenfilosofisesta todellisuuskäsityksestä, jota käsiteltiin jo aiemmin luvussa 2.3.

4.2.2.1 Pysyvät rakenteelliset järjestelmät

Kuvio 7. Topologia.

Ensimmäisellä tasolla ovat **pysyvät rakenteelliset järjestelmät**. Alkuperäisessä mallissa tätä tasoa kutsutaan *rakennetasoksi* (engl. frameworks) ja sitä kuvataan *"maailmankaikkeuden maantiedoksi ja anatomiaksi"*. Tämän kaltaisia järjestelmiä ovat esimerkiksi elektronit atomin ytimen ympärillä, geenien rakenne ja maapallon sijainti astronomisessa maailmankaikkeudessa. Pysyvien rakenteellisten järjestelmien kuvaaminen ja tunteminen on edellytys eli perusta järjestelmälliselle teoreettiselle – ja muullekin – tiedolle. Tämä edellyttää muun muassa isojen datamäärien indeksointia, kategorisointia ja luokittelua eli tiedon jäsentämistä. (Boulding 1956, 202,205) Tällaista tiedon hallintaa edellytetään kybertilannetietoisuuteen pääsemiseksi ylemmillä tasoilla.

Pysyvien rakenteellisten järjestelmien tasolla määritellään järjestelmien sisäistä ja ulkoista topologiaa (kuvio 7) eli järjestelmän sijaintia suhteessa muihin järjestelmiin (Mingers 1997, 307-308). Esimerkiksi kybertilannekeskuksen (organisaatio) tilannekeskushuone eli "War Room" (toimitila) voi sijaita tietyssä valtiossa, tietyn kaupungin alueella ja tietyssä suojatussa tilassa (Merriam-Webster 2019b). Tällöin yhden tilannehuoneen erottaa muista tilannehuoneista sijainnillaan ja sijainti luo perustan ylemmille kompleksisuustasoille kybertilannekeskusorganisaation toiminnassa. Kybertilannekeskuksen toiminnassa tason yksi järjestelmät voivat näyttäytyä organisaatiomuutoksina kybertilannekeskuksen kasvaessa, kuten uusien osastojen perustamisena toiminnan kehittämiseksi (Nair 2001, 514).

4.2.2.2 Dynaamiset järjestelmät

Kuvio 8. Dynaamiset järjestelmät.

Toisella tasolla ovat yksinkertaiset **dynaamiset järjestelmät**. Boulding kuvaa tätä tasoa nimellä *kellokoneistot* (engl. clockworks). Tasolla olevat järjestelmät ovat yksinkertaisia ja toimivat ennalta määrätyllä tavalla ja niiden keskeinen toimintaperiaate ei muutu tilanneriippuvaisesti eli kontingentisti (kuvio 8) (Nair 2001, 514).

Esimerkiksi aurinkokunta, kellot, tietokoneen komponentit, näytöt ja mekaaniset koneet kuuluvat tähän kategoriaan. Iso osa fysiikan, kemian ja taloustieteiden teorioista kuuluu myös tälle tasolle. (Boulding 1956, 202-203) Tällä kompleksisuustasolla olevat järjestelmät voidaan erottaa tasolla yksi olevista järjestelmistä toiminnan tilan aikariippuvuudella. Esimerkiksi kellon ja tietokoneen prosessorin tila muuttuu ajan kuluessa. Edelleen esimerkiksi

kybertilannehuoneeseen johtavan oven sähkölukolla voi olla vain kaksi ennalta määrättyä tilaa: auki tai kiinni. Kybertilannekeskuksen toiminnassa tämän tason ilmiö voisi olla esimerkiksi toistuva kybertilannekuvan raportointi tietyin ajallisin väliajoin johtoportaalle (Nair 2001, 514). (Mingers 1997, 307)

4.2.2.3 Hallinta- ja säätelyjärjestelmät

Kuvio 9. Termostaatti.

Kolmannella tasolla olevia järjestelmiä kutsutaan **hallinta- ja säätelyjärjestelmiksi** eli kyberneettisiksi järjestelmiksi. Kybernetiikka tutkii kyberneettisiä järjestelmiä – kuten suurta osaa kybertilannekeskuksessa käytettävistä ohjelmistoista – ja siitä kerrotaan enemmän luvussa 4.2.3. Alkuperäisessä Bouldingin mallissa taso on nimetty *termostaatiksi* (engl. thermostat). (Boulding 1956, 203)

Tämän kompleksisuustason järjestelmän erottaa tasojen 1-2 järjestelmistä informaation lähettämisen, prosessoinnin ja vastaanottamisen avulla, jotka ovat keskeisiä toiminnan edellytyksiä hallinta- ja säätelyjärjestelmille. Esimerkiksi termostaatti hallitsee ja säätelee sisäilman lämpötilaa (kuvio 9) saamansa anturitiedon avulla ja lähettää tietoa lämmitysjärjestelmille toiminnan muuttamiseksi haluttuun tasapainotilaan eli asetettuun lämpötila-arvoon. (Boulding 1956, 203; Mingers 1997, 307-308; Nair 2001, 514-515)

Esimerkkejä hallinta- ja säätelyjärjestelmätason kompleksisuuden omaavista järjestelmistä ovat ohjelmistot, ohjaus- ja valvontajärjestelmät, haittaohjelmat, heikko tekoäly, neuroverkot ja koneoppiminen. Kybertilannekeskuksessa käytettävät ohjelmistot, kuten IDS (Intrusion Detection System), IPS (Intrusion Prevention System) ja SIEM (Security Incident and Event Management). Niiden toiminta perustuu sensoreista saatavan datan tulkitsemiseen ja verkkoliikenteen hallintaan sekä hälytyksien tuottamiseen tietyntyyppisissä ennalta ohjelmoiduissa tilanteissa (taso 3). Niihin voi myös ohjelmoida ennalta määrättyjä sääntöjä toiminnan, kuten verkkoliikenteen hallitsemiseksi esimerkiksi palvelunestohyökkäyksen aikana (taso 2). Lisäksi kybertilannekeskuksissa käytettävät järjestelmät sisältävät luonnollisesti datan indeksointia, kategorisointia ja luokittelua (taso 1). Näin ollen edellisten tasojen toiminnallisuus kerrostuu aina seuraavalle kompleksisuustasolle.

4.2.2.4 Avoimet järjestelmät

Kuvio 10. Avoin järjestelmä.

Neljännellä tasolla olevia järjestelmiä kutsutaan **avoimiksi järjestelmiksi**, joka alkuperäisessä hierarkiamallissa on nimetty *solutasoksi* (engl. cell). Tällaisilla järjestelmillä on itseään ylläpitävä rakenne, jossa yhdistyvät kyky vastaanottaa, muokata ja lähettää energiaa ja materiaa (kuvio 10). Avoimen järjestelmän tehtävät on voitu jakaa järjestelmän sisäisille osille valikoidusti. Lisäksi joillakin tämän kompleksisuustason järjestelmillä on kyky monistaa itseään eli jakaantua. ”Avoimuus” perustuu järjestelmän kykyyn muokata sisäisiä prosessejaan ja suhteitaan muihin järjestelmiin palautteen perusteella sekä reagoida sopivalla tavalla tehtävänsä täyttämiseksi (Nair 2001, 514-515).

Esimerkki tilannekeskustoiminnan kannalta avoimesta järjestelmästä on ihmisen hermosolu eli neuroni, joka luo perustan kaikelle ihmisen tilannetietoisuudelle ylemmillä kompleksisuustasoilla. Kaikille hermosoluille on yhteistä solurakenne, dendriitti eli tuojahaarake, aksoni eli viejähaarake sekä hermoliitospääte. Hermoliitospäätteet mahdollistavat kemiallisen kommunikoinnin hermosolujen välillä ja solurakenne mahdollistaa materian liikkumisen solukalvon läpi. Tuoja- ja viejähaarakkeissa hermoimpulssit siirtyvät sähköisesti. (Lodish, Berk, Kaiser & Krieger 2000, 21.1)

Tulevaisuudessa esimerkiksi tietoteknisten neuroverkkojen kehittyminen ja heikon tekoälyn parantuminen vahvaksi tekoälyksi voivat johtaa teknisten kybertilannekuvajärjestelmien kehittymiseen tälle avoimien järjestelmien kompleksisuustasolle. Jo nykyaikaiset tietokoneiden suorittimet ja ohjelmoitavat digitaaliset mikropiirit saattavat yltää solutason kompleksisuuden reaaliaikavaatimuksiin eli nopeuteen. Toistaiseksi ongelmaksi on muodostunut erityisesti digitaalisten järjestelmien erilaisuus neuronien ja synapsien tiheyden, energiatehokkuuden ja resilienssin osalta verrattuna ihmisen analogisiin sähköfysiologisiin hermosolujen toimintaperiaatteisiin. Tästä syystä on pyritty mallintamaan hermosolun toimintaa analogis-digitaalisilla erittäin suurikokoisilla (engl. VLSI, Very Large Scale Integration) pii-puolijohdemikrosiruilla (Mead & Conway 1980, 3-4). Tällaisessa ratkaisussa yksittäistä hermosolun toimintaa mallintavaa, osiltaan analogista elementtiä, kutsutaan puolijohdehermosoluksi (engl. Silicon Neuron) ja tapaa jäljitellä biologista hermosolua neuromorfisuudeksi.

Esimerkiksi tietokoneiden komponentteja valmistava IBM, Qualcomm ja Intel ovat kehitelleet neuromorfisen eli ihmisaivojen hermosolujen toimintaa mukailevan prosessorin (Laine 2017). Sen etuna on tarvittavan ohjelmointityön vähäinen määrä ja virhealttiuden väheneminen muuttuviin tilanteisiin resilientisti reagoimalla. (Markoff 2013) Nykyään käytössä olevien transistorien ja komponenttien kutistaminen ei ole enää mahdollista tulevaisuudessa tarvittavan laskentatehon ja muistin määrän saavuttamiseksi. Esimerkiksi esineiden internetin on ennustettu käyttävän vuonna 2020 yli 50 miljardia sensoria. (ETN 2018) Tulevaisuudessa esimerkiksi datan ja sensorien määrän jatkuva kasvaminen voidaan mahdollisesti ratkaista neuromorfisilla komponenteilla. Toistaiseksi kehitystyö on kuitenkin vielä kesken. Esimerkiksi energiankulutus aivoissa olevissa hermosoluissa on erittäin pientä verrattuna nyt kehitettyjen suorittimien neuroneihin. Lisäksi teknologiset ratkaisut jäävät selkeästi jälkeen hitaudellaan verrattuna ihmisen hermosoluihin. (Indiveri ym. 2011, 1-2)

4.2.2.5 Sääntöperustaisesti rakentuvat järjestelmät

Kuvio 11. Elementeistä koostuva järjestelmät.

Viidennellä tasolla ovat **sääntöperustaisesti rakentuvat** eli geneettis-sosiaaliset järjestelmät. Bouldingin hierarkiamallissa tämä taso on nimetty *kasviksi* (engl. plant). Tällaisen järjestelmän erottaa edellisestä tasosta (taso 4) työn jako, erilaisuus ja tehtävien eriyttäminen yksittäisten järjestelmän elementtien välillä. Järjestelmän elementit ovat riippuvaisia toisistaan ja niillä kaikilla on oma tehtävänsä osana suuremman kokonaisuuden toiminnan varmistamista. Tämän kompleksisuustason järjestelmillä voi olla ympäristöä havainnoivia vastaanottimia, mutta ne eivät ole kovin kehittyneitä tai toimi tehokkaasti. (Boulding 1956, 204) Nimessä mainittu sääntöperustaisuus viittaa kasvuun, joka on koordinoitua siten, että osat muodostavat järkevän ja toimivan kokonaisuuden eli rakenteen (kuvio 11). (Nair 2001, 514-515)

Esimerkiksi yksittäinen kasvi rakentuu kokonaisuudeksi sääntöperustaisesti erilaisista soluista, joilla on kullakin erityinen tehtävä juuressa, runko-osassa ja lehdissä. Lisäksi kasveilla on havaittu aikaisemmin vain elämille omaksuttuja tuntoaisteja ja ympäristöstä saatavien signaalien hyödyntämistä osana puolustusvastetta, kuten kasvia syöville eläimille myrkyllisten yhdisteiden kehittämistä. Kasvien erilaisiin tehtäviin erikoistuneet solut välittävät tiedon viereisille kasvisoluille eläimiin (taso 6) verrattuna hitaasti, mutta samankaltaisten glutamaatti-aminohappojen avulla. (Toyota ym. 2018, 1112-1115) Tilannetietoisuu-

den näkökulmasta kasvit rakentuvatkin työtehtäviltään eriytyneistä soluista sääntöperustaisesti ja muodostavat kasvisolujen eli elementtien avulla verrattain hitaita kommunikointiverkostoja puolustautuakseen hyökkääjiä tai vaaraa vastaan.

Käsite **tajunta** (engl. consciousness) pitää sisällään hereillä olemisen (engl. arousal) ja tietoisuuden (engl. awareness). Hereillä oleminen tarkoittaa silmien auki olemista ja mahdollisesti pieniä motorisia toimintoja. Tietoisuus puolestaan viittaa kykyyn kokemuksille ympäristöstä, omasta kehosta, ajatuksista, muistoista, tunteista ja aikomuksista. Sääntöperustaisesti rakentuvan järjestelmän (taso 4) kompleksisuustasolla ei edellisten määritelmien mukaan ole olemassa täysimääräistä tajuntaa, sillä tietoisuus ympäristöstä puuttuu. Tällä tasolla tilannetietoisuuden astetta voi verrata ihmiseen, joka on tiedottomassa ”vegetatiivisessa” eli osittaisen aktivaation tilassa esimerkiksi aivoihin kohdistuneen onnettomuuden jälkeisestä koomasta herätessään (Jennett & Plum 1972, 734).

Vegetatiivisessa tilassa olevan ihmisen tietoisuus ei ole palautunut koomasta heräämisen jälkeen, mutta ihminen saattaa sulkea ja avata silmänsä nukkumisen sekä hereillä olon merkiksi (Owen ym. 2006, 1402). Vegetatiivisessa – tietoisuudesta poissaolevassa – tilassa oleva ihminen voi hengittää, verenkierto toimii normaalisti ja muutoinkin elintoiminnot ovat autonomisilta osiltaan normaaleja. (Working Party of the Royal College of Physicians 2003, 249) Ongelmallisen asiasta tekee sen, että tietoisuutta ei voi mitata objektiivisesti juuri millään laitteella (Laureys, Owen & Schiff 2004, 537-538). Tilannetietoisuuden näkökulmasta tällä kompleksisuustasolla olevat järjestelmät ovatkin ”hereillä” ja suorittavat pieniä motorisia toimintoja, mutta eivät omaa tietoisuutta.

4.2.2.6 Ympäristöstä tietoiset järjestelmät

Kuvio 12. Ympäristöstä tietoiset järjestelmät.

Kuudennella tasolla ovat **ympäristöstä tietoiset järjestelmät**, joita on alkuperäisessä mallissa nimetty *eläimiksi* (engl. plant). Ympäristöstä tietoinen järjestelmä on ominaisuuksiltaan tavoitehakuinen, itsetietoinen ja sillä on suuri määrä ympäristöä havainnoivia vastaanottimia. Järjestelmä toimii ympäristöä havaiten holistisesti eli kokonaisvaltaisesti siten, että moni ympäristön tekijä muodostaa yhtenäisen tilannekuvan, jonka perusteella järjestelmä muuttaa toimintatapojaan. (Boulding 1956, 204; Read 1999, 852) Ympäristöstä tietoiset järjestelmät muodostavat

yksityiskohtaisen tietoisuuden ympäristöstä hankitun tiedon avulla, joka organisoidaan tietorakenteiksi ja tilannekuvaksi (Nair 2001, 514).

Eläimillä ja ihmisillä hermojärjestelmä eli hermosoluista ja hermokudoksista muodostuva kokonaisuus muodostaa esimerkin ympäristöstä tietoisesta järjestelmästä (taso 6), jonka perusteella dataa vastaanotetaan silmissä (kuvio 12), korvissa ja muissa aistielimissä. Vastaanotetusta datasta muodostetaan selkäytimessä – selkärankaisilla lisäksi aivoissa – kokonaiskuva ja käyttäytyminen sovitetaan sen perusteella ympäristöön tavoitehakuisesti. Hermoston tehtävä on koordinoida eli säädellä vasteita ärsykkeisiin, ohjata käyttäytymistä sekä olla tietoisuuden toteutumisen edellytyksenä. (Boulding 1956, 204; Read 1999, 852) Toisin kuin edellisellä sääntöperustaisesti rakentuvien järjestelmien tasolla (taso 5), eläimet ja ihmiset vaativat nopeita ja pitkän kantaman omaavia hermoverkostoja, jolla aistit yhdistetään kehossa ja hermokeskuksissa ympäristön kannalta järkeväksi vasteeksi. (Toyota ym. 2018, 1112)

Ympäristöstä tietoiset järjestelmät omaavat tietoisuuden lisäksi tunteita ja älykkyyttä vaihtelevasti. Nämä ominaisuudet eivät ole ominaisia vain inhimillisille järjestelmille (taso 7), kuten on aikaisemmin luultu (Pirkkalainen 2012). Aivokuoren uloimman osan puuttuminen muilla, kuin ihmisillä ei estä ympäristöstä tietoisten järjestelmien kykyä tunteisiin. Esimerkiksi kaikilla nisäkkäillä, linnuilla ja monilla muilla olennoilla on neurologiset valmiudet tietoisuuteen ja tunteisiin. (Low 2012)

4.2.2.7 Inhimilliset järjestelmät

Kuvio 13. Inhimilliset järjestelmät.

Seitsemännellä tasolla ovat **inhimilliset järjestelmät**. Boulding nimeää tämän kompleksisuustason *ihmiseksi* (engl. human) ja sen erottaa muista tasoista kyky tuottaa ja ymmärtää symboleita ja puhuttuja kieliä sekä ymmärtää asioiden välisiä suhteita kehittyneesti (kuvio 13). Lisäksi ihmisillä – inhimillisinä järjestelminä – on kehittyneempi kuva ajasta, kuten tietoisuus tulevasta kuolemasta ja elämän rajallisuudesta. (Boulding 1956, 204-205)

Kuudennella tasolla olevilla järjestelmillä on aikakäsitys, mutta se perustuu kellon sijasta luonnon muutoksiin eli biologisiin sykleihin, kuten päivän ja yön valon määrän vaihteluihin tai vuodenaikojen vaihteluihin (Gallistel 1989, 156-157; Richelle & Lejeune 1980, 3). Kä-

dellisenä inhimillisenä järjestelmänä ihminen kykenee monista muista järjestelmistä poiketen luomaan työkaluja, kirjoittamaan muistiin asioita ja kehittämään teknologiaa. (Boulding 1956, 204-205) Erään tutkimuksen mukaan ihmisaivojen hermosolujen aktiivisuus olisi geneettisten muutosten vuoksi korkeampi verrattuna kädellisiin eläimiin, kun puolestaan sisäelinten genetiikka on hyvin saman tyyppistä ihmisessä ja eläimessä (Cáceres ym. 2003, 13030).

Esimerkiksi tilannekeskuspäivystäjä kykenee ihmisenä käyttämään näppäimistöä käsillään ja kommunikoimaan ajatuksiaan muille työntekijöille puheen avulla. Kädentaidot mahdollistavat asioiden tallentamisen muistiin esimerkiksi näppäimistöllä kirjoittaen ja hiirtä tarkasti käyttäen. Lisäksi kybertilannekeskuksessa työskentelevillä on puhutun kielen lisäksi ohjelmointikielten ja koneidenkäytön osaamista, joilla he voivat antaa koneille komentoja ja käskyjä. Puheen avulla tilannekeskuspäivystäjä kykenee jakamaan ajatuksiaan tarkasti ja monipuolisesti muille samassa tilassa kuuloetäisyydellä tai etäyhteyden kautta toimiville inhimillisille järjestelmille. Nämä tekijät erottavat ympäristöstä tietoiset järjestelmät inhimillisistä järjestelmistä. Samoja tekijöitä myös edellytetään kybertilannekuvan muodostumiseksi inhimillisissä järjestelmissä.

4.2.2.8 Sosiaaliset järjestelmät

Kuvio 14. Sosiaaliset järjestelmät.

Kahdeksannella tasolla ovat **sosiaaliset järjestelmät**, jotka erottaa muista tasoista roolijakoisuuden, kommunikoinnin ja ihmissuhteiden avulla. Rooli voi olla esimerkiksi työtehtävä, jonka takana vaikuttaa ihmisen persoonallisuus ja monet muut kompleksiset tekijät muilla tasoilla, esimerkiksi tavoitteellisuus. Kommunikointi mahdollistaa ihmissuhteiden muodostumisen ja jaetun tilannekuvan muodostumisen (kuvio 14) (Boulding 1956, 205)

Sosiaaliset järjestelmät sisältävät viestejä, tarkoitushakuisuutta, arvoja, historiallista tietoa, taidetta ja tunteita. (Boulding 1956, 205) Hyvänä esimerkkinä tämän tason ilmiöstä on organisaatio, joka voidaan määritellä neljällä tavalla: Tavoitteellisuuden ja tehokkuuden, nykytilan säilyttämisen, organisaation ja sen toimintaympäristön välisen vuorovaikutuksen sekä organisaatioon liitettävien käsitysten kautta (Harisalo 2008, 17-19).

Esimerkiksi kybertilannekeskuksessa – organisaationa – toimii tilannekeskuspäivystäjiä, tilannekoordinaattoreita, asiantuntijoita, ohjelmistokehittäjiä, ylläpitäjiä ja johtajia. Tällä kokonaisuudella on tehtävä, tavoitteita ja arvoja. Jokaisella on oma roolinsa osana organisaation tehtävän täyttämistä. Organisaation työntekijät toimivat rooleissa, joiden hoitamiseen vaikuttaa ihmisen persoonallisuuden, osaamisen ja kokemuksien lisäksi kaikki edellisten kompleksisuustasojen ominaisuudet: organisaation tehtävä ja tavoitteet (taso 8), kyky kommunikointiin puheella, kädentaitoihin ja monimutkaisten suhteiden ymmärtämiseen (taso 7), tietoisuuteen ympäristöstä kokonaisvaltaisesti erikoistuneiden aistien avulla (taso 6) ja säännönmukaisuuksiin järjestelmän osien työnjaossa ja yhteyksissä toisiinsa (taso 5), kykyyn itseään ylläpitävien rakenteiden luomiseen sekä mahdollisuuteen energian ja materian vaihdantaan (taso 4), järjestelmän hallinta- ja säätelymekanismeihin (taso 3), mekaanisiin toimintoihin (taso 2) ja sijaintiin suhteessa muihin järjestelmiin (taso 1).

4.2.2.9 Toistaiseksi tuntemattomat järjestelmät

Kuvio 15. Toistaiseksi tuntemattomat järjestelmät.

Yhdeksännellä tasolla ovat **toistaiseksi tuntemattomat järjestelmät**. Tällaisia järjestelmiä Boulding kategorisoi todella korkean tason järjestelmiksi (engl. transcendental) (Read 1999, 1333). Tällaisista järjestelmistä ei ole nykytiedon valossa esimerkkejä, mutta tieteen kehittyessä on mahdollista löytää kompleksisuustasoltaan myös sosiaalisia järjestelmiä (taso 8) korkeampia järjestelmiä, joihin tällä tasolla on etukäteen varauduttu (kuvio 15). (Boulding 1956, 205)

Yhtä kaikki järjestelmäteorian johdannaisena Bouldingin mallin avulla kyetään kuvaamaan teoreettisesti kybertilannekeskuksiin järjestelminä sisältyvien järjestelmien eli elementtien keskinäisiä kompleksisuustasojen eroja ja yhteyksiä. Mallissa yhdistyvät kybertilannekeskuksen (taso 8) eli ihmisten (taso 7) yhteistoiminnan, havaitsemiskyvyn (taso 6), työnjaon (taso 5), kommunikoinnin ja vuorovaikutuksen (taso 4), kyberneettisten hallinta- ja säätelyjärjestelmien (taso 3), ajan (taso 2) ja paikan (taso 1) kompleksisuudet. Työntekijöiden toiminnan organisointi tehokkaasti ja vaikuttavasti (taso 8) on huomattavasti kompleksisempaa, kuin esimerkiksi teknisten järjestelmien (tasot 1-3) säätäminen toimimaan tehokkaasti ja vaikuttavasti. Lisäksi teknisillä järjestelmillä (tasot 1-3) ei kyetä ratkaisemaan ihmisistä

(tasot 8 ja 9) johtuvia haasteita, sillä ihmisaivojen kompleksisuutta – ylivoimaisuutta luovuuteen sekä ajan ja suhteiden tunnistamiseen – ei voida toistaiseksi korvata millään teknologisilla ratkaisuilla. Ihmisen kybertilannetietoisuuden edellytyksenä kuitenkin on alempien järjestelmien oikeanlainen toiminta, sillä tilannetietoisuus kumuloituu alempien järjestelmien kautta ihmisille ja organisaatioille. Työntekijät ovat kybertilannekeskuksen kompleksisin ja tärkein voimavara, mutta ilman teknologisia ratkaisuja kybertilannekuvan muodostaminen ei ole mahdollista. Esimerkiksi ilman kyberavaruuden aisteja eli antureita ihminen ei kykene saamaan tilannetietoja eikä muodostamaan tilannekuvaa kyberavaruudessa vallitsevasta tilanteesta. Toisin sanoen kybertilannekeskuksen toiminta ei ole mahdollista ilman teknisiä tilannekuvajärjestelmiä, kuten hallinta- ja säätelyjärjestelmiä (taso 3), sillä kybertoiminta tapahtuu tällä ihmisen aistielinten ulkopuolisella kyberalueella.

Bouldingin mallin avulla havaitaan, että tietoisuus muodostuu korkeammilla kompleksisuustasoilla (tasot kuudesta ylöspäin), mutta vaatii alemmat tasot muodostuakseen. Nykyteknologialla ylletään tasojen 1-3 ja osittain 4 alueille ihmisestä riippumattoman ”tilannetietoisuuden” tavoittelussa. Tästä syystä ihmistä tullaan vielä pitkään tarvitsemaan tietoisuuden luomisessa. Teknisillä järjestelmillä voidaan selkeästi tukea inhimillisten järjestelmien eli työntekijöiden toimintaa tilanteen ja tietoisuuden yhdistämiseksi tilannetietoisuudeksi. Tästä syystä onkin tärkeää kiinnittää huomiota eri kompleksisuustasoilla olevien järjestelmien synergiaetujen toteutumiseen ja toimintatapojen kehittämiseen eri tasot huomioiden. Näin voidaan parantaa kybertilannetietoa luovan kybertilannekeskuksen vaikutusta organisaation kyberresilienssiin.

4.2.3 Kybernetiikka eli kontrolli ja säätö resilienssin näkökulmasta

Edellä esitetty tilannetietoisuuden hierarkkinen malli kuvaa tilannetietoisuutta eritasoisten järjestelmien ominaisuutena. Organisaation kyberresilienssin ja tilannetietoisuuden suhteen selventämiseksi on tässä tutkimuksessa välttämätöntä selittää, miten tilannetietoisuus vaikuttaa resilienssiin. Toisin sanoen, miten kybertilannekeskustoiminta vaikuttaa organisaation kyberresilienssiin.

Täysin valmiin mallin puuttuessa on luotu useammasta teoreettisesta mallista yhdistelmä, joka selittää kybertilannetietoisuuden ja kyberresilienssin suhdetta. Mallissa on yhdistelty

järjestelmäteoriapohjaisia kyberneettisiä teoreettisia viitekehyksiä yhdeksi kokonaisuudeksi, jota kutsutaan **kybertilannekeskuksen resilienssimalliksi**.

Malli sisältää järjestelmäteorian mukaisen kyberneettisen järjestelmän toimintaperiaatteen (von Bertalanffy 1968, 160-163), organisationaalisen resilienssi- ja vastemallin (Burnard & Bhamra 2011), tilannetietoisuuden mallin (Endsley 1995), organisationaalisen resilienssin hallinnan prosessimallin (Seville ym. 2008), verkostojen resilienssimallin (Pettit ym. 2010) ja varautumiseen liittyvän yhdistetyn jatkuvuus- ja toipumissuunnittelun mallin (Sahebjamnia, Torabi & Mansouri 2015). Lisäksi mallissa hyödynnetään ISO/IEC tietotekniikan jatkuvuusstandardin 27031:2011 periaatteita ja sanastoa (International Organization for Standardization 2011).

4.2.3.1 Yleistä kybernetiikasta ja resilienssistä

Kuvio 16. Kyberneettisen järjestelmän toimintaperiaate.

Kybernetiikka on järjestelmäteorian johdannaistiede viestintä- ja hallintajärjestelmille, jossa järjestelmät mukautuvat ympäristön muutoksiin saamansa palautteen pohjalta (Lemak 2004, 1319; Wiener 1948, 11). Kuviossa 16 esitetään kyberneettisen järjestelmän elementit: vastaanotin, päätöksentekoelin ja vaikutuselin. Kyberneettinen prosessi muodostuu ärsykkeestä (engl. stimulus), joka vaikuttaa vastaanottimeen (engl. receptor). Vastaanottimen havaitsemat tilannetiedot vaikuttavat päätöksentekoelimeen (engl. control apparatus), jossa tilannekuvan pohjalta muodostetaan päätös vasteesta. Varsinainen vaste (engl. response) tuotetaan vaikutuselimellä (engl. effector) ympäristöön. Tämän jälkeen kerätään palautetta ympäristöstä tilannetietojen muodossa. Tätä prosessia kutsutaan palautesilmukaksi (engl. feedback). (von Bertalanffy 1968, 160-163)

Mallin ajatus on, että palaute mahdollistaa säätöprosessin, jossa järjestelmä voi mukautua ympäristöön ja päästä tavoitteisiinsa. Ideana on järjestelmän itsesäätelymekanismi, joka ohjaa sen toimintaa kohti tasapainotilaa. Tällaisia mekanismeja on tutkittu paljon esimerkiksi biologiassa ja sosiaalitieteissä (Boulding 1956, 203). Varsinaista päätöksentekoprosessia ei mallissa kuvata. Monet tutkijat ovatkin muodostaneet kybernetiikan idean pohjalle omia

ratkaisujaan, kuten tässäkin tutkimuksessa. Ratkaisu on yhdistelmä aiemmin luotuja teoreettisia malleja, jotka esitellään seuraavissa alaluvuissa. (von Bertalanffy 1968, 161)

4.2.3.2 Resilienssin aiempi tutkimuskirjallisuus

1800-luvulta lähtien resilienssillä on tarkoitettu ihmisen ominaisuutta selviytyä psykologisista haasteista ja fysiologiseen stressiin johtavista asioista. Resilienssitutkimus on keskittynyt positiivisten tulosten tutkimukseen ja niihin johtaviin asioihin esimerkiksi sairauksien tutkimisen sijasta. Resilienssiä parantavia henkilökohtaisia tekijöitä ovat ihmisillä muun muassa optimismi, älykkyys, luovuus, huumori, kokemuksellisuus, yhtenäisyys ja erilaisuus. Myös tietyt henkilökohtaiset taidot, kuten sosiaaliset kyvyt, koulutus ja keskimääräistä parempi muisti ovat tekijöitä, jotka parantavat resilienssiä ja auttavat selviytymään haitallisista tapahtumista. Ympäristöllisistä tekijöistä resilienssin kannalta tärkeitä ovat erityisesti koettu sosiaalinen tuki, yhteenkuuluvuuden tunne ja tärkeät elämäntapahtumat. Resilienssin tutkimisen ja kehityksen kannalta keskeisiä tekijöitä ovat ihmisen ja ympäristön välillä tapahtuvan dynaamisen vuorovaikutuksen, kokonaisvaltaisen holistisen näkökulman, tieteidenvälisen toimialarajat ylittävien työyhteisöiden ja koulutusten merkityksen korostaminen. (Southwick & Charney 2018; Tusaie & Dyer 2004, 3-7)

Viimeisen 50 vuoden aikana resilienssin tutkimus ja soveltaminen on laajentunut yksittäisen ihmisen tutkimisesta vuorovaikutuksien, sosiaalitieteiden, ekologian, teknologian ja turvallisuuden tutkimukseen.

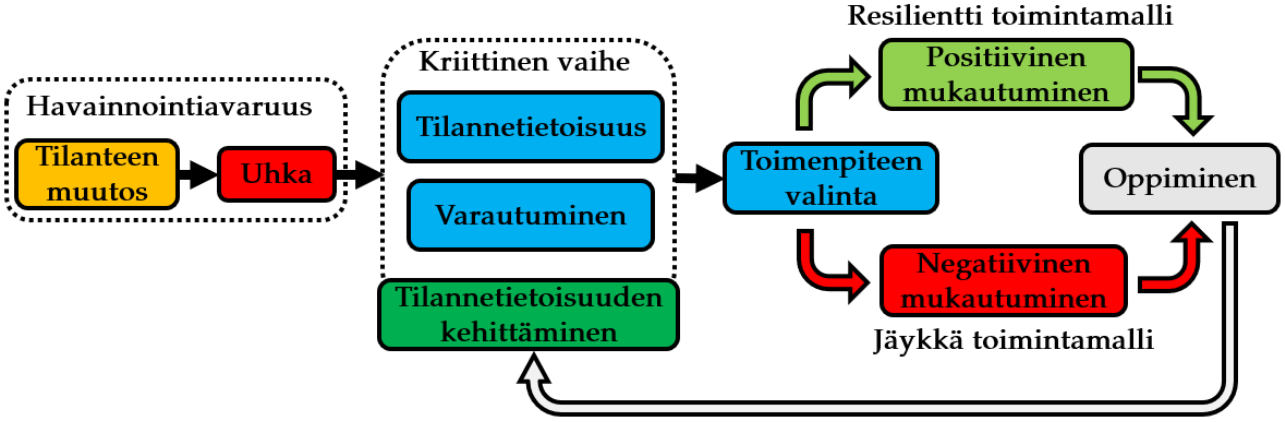
Ekologiassa tutkitaan ekosysteemien kykyä selvitä ympäristöä häiritsevistä muutoksista, kuten ilmastonmuutoksesta (Holling 1973; Stevens-Rumann ym. 2018). Teknologian alueilla tutkitaan esimerkiksi rakennusmateriaalien kestävyyttä ja joustavuutta tarpeellisen lujuuden säilyttämiseksi maanjäristysten tai muiden haitallisten tapahtumien varalle (Sharma, Tabandeh & Gardoni 2018; Woods 2015, 4). Sosiaalitieteissä tutkitaan ihmisistä koostuvien yhteisöjen kykyä selvitä ympäristön muutoksista ja jatkaa toimintaansa. Tästä eräänä esimerkki on Kreikan talouskriisin vaikutusten tutkiminen (Apostolopoulos, Newbery & Gkartzios 2018). Turvallisuuden tutkimuksen näkökulmasta on tutkittu esimerkiksi yhteiskunnan kokonaisresilienssiä. Kokonaisresilienssissä on kyse poliittisen järjestelmän, yhteisöjen ja yksilöiden kyvystä jatkaa toimintaansa häiriö- ja kriisitilanteissa sekä uudistua demokraattisia kanavia käyttäen. (Hyvönen ym. 2019, 24)

Tyypillisesti tutkimuskirjallisuudessa resilienssi jaetaan haitallisen tapahtuman vaiheiden mukaisesti iskunkestävyyteen ja sopeutumiseen. (Hyvönen ym. 2019, 16-18; Tierney 2014, 169-173)

Iskunkestävyydellä kuvataan haitallisen tapahtuman jälkeistä aikaa eli järjestelmän mukautumista iskuun. Iskunkestävyys jaetaan vastustuskykyisyyteen (engl. robustness) ja korvattavuuteen (engl. redundancy). Vastustuskyky tarkoittaa käytännössä kykyä vastustaa kyberuhan toteutumisen aikaansaamaa toimintotason laskua. Korvattavuus tarkoittaa esimerkiksi elintärkeiden toimintojen kahdentamista erilaisilla varajärjestelmillä. Tällöin toimintakyvyttömät järjestelmät ovat korvattavissa toipumisen ajaksi ja organisaation elintärkeät toiminnot kyetään pitämään toiminnassa. (Hyvönen ym. 2019, 16-18; Tierney 2014, 169-173)

Sopeutuminen puolestaan kuvaa tapahtuman jälkeistä toipumista ja järjestelmän kykyä edistää palautumista normaaliin toimintotasoon. Sopeutuminen koostuu resurssien hyödyntämisestä (engl. resourcefulness) ja niiden käytön nopeudesta alentuneen resilienssin palauttamiseksi. Esimerkiksi kybertilannekeskuksen henkilökunnan kokemus, taidot ja kyvyt vaikuttavat ymmärrykseen tilannetta parantavista oikeista ja viisaista päätöksistä. Tämä vaikuttaa toipumisen nopeuteen. Vastaavasti esimerkiksi tilannetietojen laajuus ja tilannetietoisuusprosessin nopeus havainnon ja korjaavien toimenpiteiden välillä vaikuttavat yhteenlaskettuun häiriöaikaan. (Hyvönen ym. 2019, 16-18; Tierney 2014, 169-173)

4.2.3.3 Organisationaalinen resilienssi- ja vastemalli



Kuvio 17. Organisationaalisen resilienssin vastemalli. (Burnard & Bhamra, 2011)

Organisationaalisen resilienssin malli on kyberneettinen palautesilmukallinen graafinen konsepti, joka yhdistää havaitsemis- ja vastekyvyn toisiinsa.

Mallin mukaan organisationaalinen resilienssi tarkoittaa järjestelmän kykyä vastata ja mukautua ympäristössä tapahtuviin muutoksiin. Toisin sanoen organisaatiolla on kykyä selvitä tuntemattomista tulevaisuuden haasteista. Organisationaalisessa resilienssissä organisaatiolla on kyky kestää epäjatkuvuuksia. Organisaation resilienssiä voidaan parantaa resurssien hyödyntämisen joustavuudella ja mukautumiskykyisyydellä palautesilmukan avulla. Resilienssin taso perustuu prosesseihin ja resursseihin, jotka tuottavat tietämystä ja kasvua organisaatiolle. (Burnard & Bhamra 2011, 5583 ja 5587)

Mallissa (kuvio 17) organisaation tilannevasteen toteuttaminen jaetaan negatiiviseen ja positiiviseen mukautumiseen. Negatiivinen mukautuminen (kuviossa punaisella) on jäykkä ja olettaa, että uhat ympäristössä johtavat väistämättä epäsuotuisiin tapahtumiin ja jäykkiin keskitetyn johtamisen organisaatiorakenteisiin. Negatiivinen mukautuminen johtaa kehittymisen ja selviytymisen rajoittamiseen, eikä siten paranna resilienssiä. Negatiivista mukautumista tulee välttää.

Positiivisessa mukautumisessa organisaatiot kykenevät mukautumaan kompleksiseen toimintaympäristöön, säilyttämään toimintakykynsä merkittävistä häiriöistä huolimatta ja toipumaan odottamattomista tapahtumista oppimalla. Tämä tapahtuu palautesilmukan avulla, joka kuvaa toiminnan jatkuvaa kehittämistä. Mallin mukaan organisaation positiivista mukautumista hallitaan häiriöiden havaitsemiskyvyllä, joka on edellytys palautteen saamiseksi organisaation kaikille tahoille ja järjestelemille. Uhkien tunnistaminen tehokkaasti on tällöin tärkeää. (Burnard & Bhamra 2011, 5588 ja 5589)

Uhkaavan tapahtuman havaitseminen muodostuu tilannetietoisuudesta ja tapahtumaan varautumisesta. Havaitsemisvaihe on resilienssin kannalta kriittinen ja molemmat tekijät vaaditaan tilannevasteen mahdollistamiseksi. Tilannetietoisuus muodostuu organisaatiossa olevasta tietämyksestä ja organisaation sisäisten sekä ulkoisten olosuhteiden tilannetiedoista. Tämä pitää sisällään esimerkiksi organisaation kyvykkyyksien, haavoittuvuuksien ja nykytilan tuntemuksen.

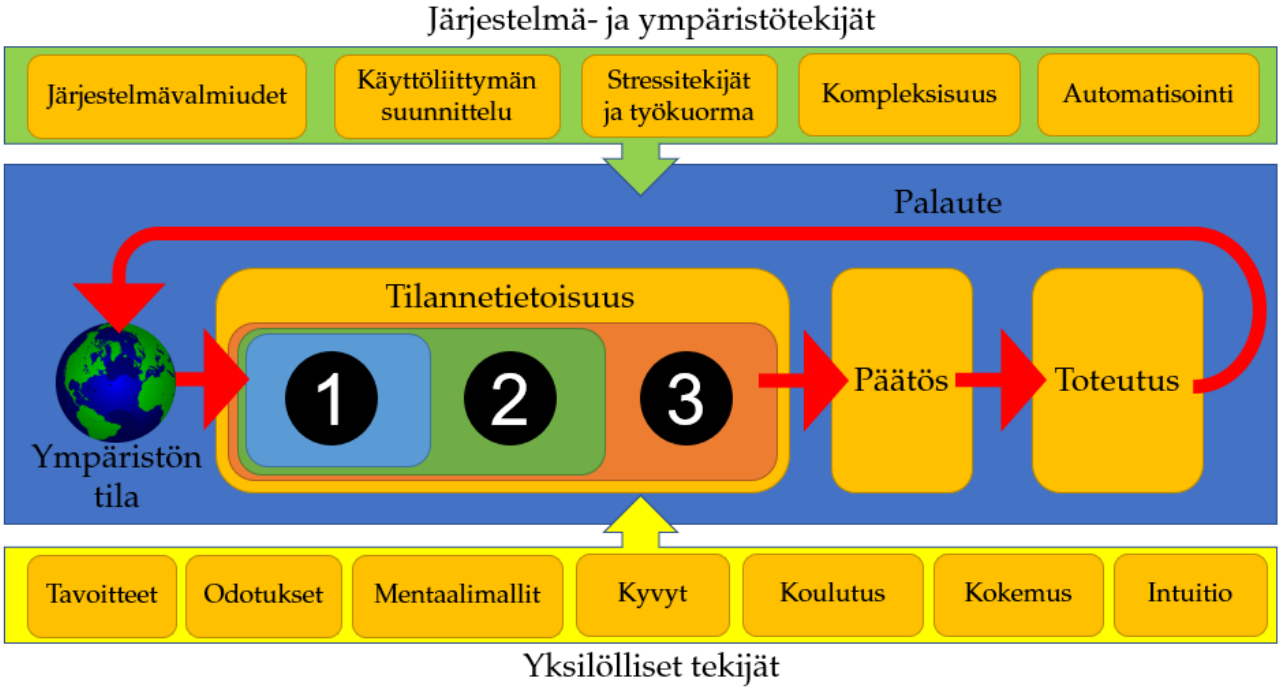
Tapahtumaan varautuminen muodostuu tehokkaista prosesseista mobilisoida etukäteen varautumalla kerrytetyt resurssit ympäristön muutosvoimiin mukautumiseksi tilannevasteen muodossa. Toiminnan jatkuvuutta uhkaavan haitallisen tapahtuman kohdatessa organisaatio pyrkii mahdollisimman nopeasti palauttamaan järjestyksen ja käyttöönottamaan tarpeelliset resurssit tilanteen hallitsemiseksi. Tätä edistävät päätöksenteon hajauttaminen,

muodollisuuden minimointi, orgnisaatiorajojen mataluus, paikallinen toimintakulttuuri ja yhteistyöverkostot. Näin teknologinen ja inhimillinen pääoma tuottaa organisaatiolle mahdollisimman suurta resilienssiä. (Burnard & Bhamra 2011, 5589-5593)

4.2.3.4 Tilannetietoisuuden malli

Tilannetietoisuuden mallin mukaan tilannetietoisuus tarkoittaa ympäristön muutosten käsittämistä tietyssä ajassa ja paikassa. Lisäksi se on ymmärrystä muutosten merkityksestä ja lähitulevaisuudessa tapahtuvien muutosten ennustamista. (Endsley 1995, 36)

Tilannetietoisuuden malli on dynaamisessa ympäristössä inhimillistä päätöksentekoa kuvaava malli. Sen mukaan pelkkä tilannetietojen vastaanottaminen ei riitä, vaan päätöksenteon erinomaisuuteen vaaditaan tilanteen ymmärtämistä. Päätöksenteko ja järjestelmän kyvykkyyksien käyttäminen nojaavat tilannetietoisuuteen. Tilannetietoisuus on kuitenkin itsessään näistä erillään.



Kuvio 18. Tilannetietoisuuden malli (Endsley, 1995, 35). Tilannetietoisuus on tietämyksen tila, joka saavutetaan tilanteen arviointiprosessissa (numerot 1-3). Tämän perusteella tehdään tilanteenmukainen päätös ja toteutetaan toimenpiteet.

Tilannetietoisuuden mallia hyödynnettiin alun perin jo 1. maalimansodassa sotalentäjien tarkan ja oikean tilannetietoisuuden tutkimuksessa. Myöhemmin mallia on hyödynnetty muun muassa lennonjohdossa, isoissa teollisuusjärjestelmissä ja turvallisuustoimijoiden,

kuten poliisin, pelastajien ja sotilaiden operatiivisessa toiminnassa. Näissä havainnoija pyrkii havainnoimaan ympäristöstä vihjeitä tulevasta muutoksesta, joka vaikuttaa päätöksentekoon. Mallin mukaan havaintovirheet ovat yleisiä. Tilannetietoisuuden tarve on aina läsnä, mutta sen saavuttamisesta tulee vaikeampaa kompleksisuuden ja muutosvoimien määrän kasvaessa. Hyvätasoisella tilannetietosuudellakin voi tehdä väärän päätöksen vähäisen harjoittelun, huonojen toimintatapojen tai taktiikan takia. (Endsley 1995, 32-36)

Varsinainen päätöksenteon malli on graafinen (kuvio 18). Ensimmäisessä vaiheessa (1) ympäristön merkityksellisten tilannetietojen havaitsemiskyky muodostaa pohjan tilannetietoisuudelle. Tämä voi tapahtua esimerkiksi ihmisaistein tai erillisten antureiden avulla. Tässä vaiheessa ympäristön elementtien tilaa, ominaisuuksia ja muutoksia havaitaan datana. Toisessa vaiheessa (2) hajallaan olevat tilannetiedot yhdistetään synteesillä toisiinsa ja havainnoija muodostaa kokonaisvaltaisen tilannekuvan elementtien muutoksen merkittävyydestä omiin tavoitteisiinsa suhteutettuna. Tavoitteisiin suhteuttaminen on mittari kokeneesta päätöksentekijästä. Kolmannessa vaiheessa (3) muutoksien ennustamiskyky muodostaa tilanneymmärryksen. Näin ollen kolmas vaihe saavutetaan ensimmäisen ja toisen vaiheen pohjalta. (Endsley 1995, 35-37)

Tilannetietoisuuden saavuttaminen vaatii aikaa. Se on keskeinen tekijä määrittelemässä tilannetietoisuutta nykyhetken ja tulevaisuuden osalta. Tämän lisäksi paikka ja sen muutokset ovat keskeisiä tekijöitä tilannetietoisuuden muodostumisessa, sillä elementtien muutos havaitaan yleensä paikan muutoksina.

Ihmisryhmän tilannetietoisuuden taso määritellään ryhmän yksilöiden tilannetietoisuuksien muodostamana kokonaisuutena. Ihannetilanteessa ryhmän jäsenten tilannetietoisuuksien välillä vallitsee tasapaino, jolloin jokainen tuntee tilanteesta määritellyn osa-alueen. Yhdelle kasaantunut tilannetietoisuus muiden ollessa tilannetiedottomia ei ole mallin mukaan tehokasta. Jokaisen jäsenen täytyy tuntea oman vastuualueensa vaatimukset tilannetietoisuuden suuntaamiseksi.

Tietoa jaetaan ryhmäläisten välillä puheviestinnällä. Se parantaa ryhmän tilannetietoisuuden tasoa. Vastaavaan lopputulokseen voi päästä myös vähäisellä puheviestinnällä, jos ryhmäläisten mentaalimallit ovat yhteneväisiä. Mentaalimalli tarkoittaa yksilöllistä tietämyk-

sen muodostumisen tapaa ihmismielessä. Mentaalimallia päivitetään ja hyödynnetään havaintojen sekä tilanteiden tulkinnassa ympäristöön verraten. (Åhman & Gustafsberg 2017, 14; Endsley 1995, 38)

Tilannetietoisuus vaikuttaa päätöksentekomallin valintaan. Valitun päätöksentekomallin ollessa väärä ihminen tyypillisesti epäonnistuu ongelmanratkaisussa, jolloin hyvän tilannetietoisuuden tarve korostuu. Tilannetietoisuus on tekijä, joka lisää todennäköisyyttä hyvään päätökseen, mutta ei välttämättä takaa sitä. (Endsley 1995, 39-40)

Tilannetietoisuuteen vaikuttavat yksilölliset tekijät sekä järjestelmä- ja ympäristötekijät.

Yksilöllisiä tilannetietoisuuteen vaikuttavia tekijöitä ovat ennakoiminen, huomion kiinnittäminen, havaintokyky, työmuistin kapasiteetti, pitkäaikaismuistin hyödyntäminen, automaattiset toimintatavat ja tavoitteet. (Endsley 1995, 40-49)

Järjestelmä- ja ympäristötekijöitä ovat muun muassa käyttöliittymien suunnittelu tukemaan yksilöllisiä tekijöitä monilta osin. Näitä ovat muun muassa kerralla esitettävän datan määrä (työmuistikapasiteetti), stressitekijöiden määrä (häly, työtehtävien samankaltaisuus, epävarmuus ja aikapaine), työkuorma (ihannetilassa tilannetietoisuus on korkealla tasolla ja työkuorma matalalla tasolla), järjestelmien monimutkaisuus (liikkuvien osien, vuorovaikutusten ja muutostiheyden määrä) ja rutiinien määrä (rutiineihin toimintansa tukevan havainnoijan kyky huomata järjestelmän virheitä heikentyy). (Endsley 1995, 49-54)

Tilannetietoisuudessa tapahtuvia virheitä kutsutaan havaintoharhoiksi. Ne ovat kuin suodattimia todellisuudesta. Niiltä ei voi täysin välttyä, mutta havaintoharhoja tiedostamalla voidaan tukea parempaa tilannetietoisuuden kehittymistä. Havaintoharhoja luovat muun muassa valikoiva tarkkaavaisuus (engl. selective attention), ensivaikutelma, (engl. diagnosis bias), hahmotus (engl. pattern recognition), vahvistusilluusio (engl. confirmation bias), menetyksen vastenmielisyys (engl. commitment confirmation), ryhmän sisäinen sortaminen (engl. stereotype threat), ankkurointivaikutus (engl. anchoring bias) ja ryhmäajattelu (engl. group think). (Endsley 1995, 54-57; Ross 2014, 57, 59, 61, 63, 66, 67, 69 ja 71)

4.2.3.5 Resilienssin hallinnan helpotettu prosessimalli

Resilienssin hallinnan helpotettu prosessi on malli organisationaalisen päivittäisen resilienssin parantamiseksi. Päivittäisen toiminnan kehittämisen nähdään palvelevan parhaiten myös kriisitilanteita.

Mallin mukaan resilienssi määritellään koostuvan tilannetietoisuudesta, keskeisten haavoittuvuuksien hallinnasta ja mukautumiskyvystä kompleksisessa, muuttuvassa ja keskinäisriippuvaisessa ympäristössä. Mallin ideana on, että tunnettujen haavoittuvuuksien lisäksi organisaatioiden tulee pystyä toimimaan luotettavasti myös ennakoimattomissa häiriötilanteissa. Lisäksi mallin tavoitteena on resilienssin muuttaminen konkreettisiksi käytännöllisiksi ja tehokkaiksi resilienssiä kasvattaviksi rakenteiksi. (Seville ym. 2008, 81)

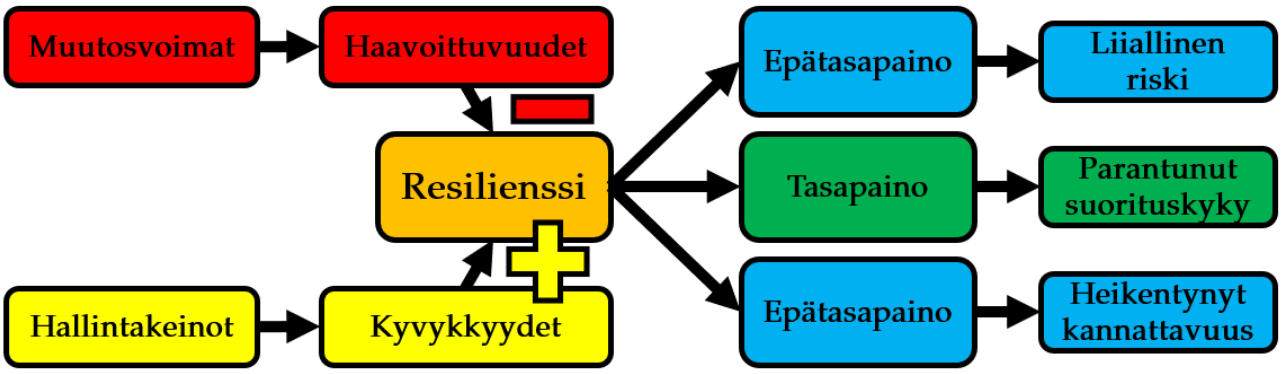
Tilanneymmärryksen osalta malli painottaa organisaatioiden välisen **tilannetietoisuuden** kehittämistä, sillä organisaatiot ovat toiminnassaan riippuvaisia toisistaan. Organisaation ei tulisi toimia yksin, vaan olla aktiivisia verkostoitumaan paremman tilannetietoisuuden saavuttamiseksi. Nykytilan kartoitus, käytettävissä olevien resurssien tunnistaminen, sidosryhmien odotukset ja kriisien vaikutusanalyysit ovat osa tilannetietoisuuden kehittämistä. Malli painottaa haastatteluiden, kyselyiden, harjoittelun ja skenaariotoiminnan tärkeyttä uhkien ja niiden seurausten arvioinnissa. (Seville ym. 2008, 82-85)

Tyypillisiä syitä organisaation epäonnistumiseen resilienssin hallinnassa on **keskeisten haavoittuvuuksien hallinnan** epäonnistuminen. Näitä ovat esimerkiksi taloudelliset vaikeudet epävarmuuden keskellä ja arvoketjujen riippuvuussuhteiden aiheuttamat ongelmat. Mallin mukaan resilientti organisaatio tekee toiminnastaan haavoittuvuusarvion ja tunnistaa elintärkeät operatiiviset, strategiset ja hallinnolliset toiminnot sisäisestä (suoraan hallittavista) ja ulkoisesta (ei suoraa vaikutusvaltaa) näkökulmasta. Esimerkkinä edellisistä ovat työsopimukset (sisäinen) ja ulkoistetut palvelut (ulkoinen). Tunnistetut haavoittuvuudet järjestetään kriittisyyden ja varautumisasteen perusteella haavoittuvuusmatriisiin, johon kuvataan alttius arvioidun haavoittuvuuden toteutumiselle. Tämän toiminnan tulisi olla sisäänrakennettuna organisaation jatkuviin prosesseihin. (Seville ym. 2008, 83 ja 85-87)

Mukautumiskyky on kykyä muokata strategiaa, toimintatapoja, hallintajärjestelmiä, hallintorakenteita ja päätöksentekoa tukevia kyvykkyyksiä. Tämä tarkoittaa kykyä joustaa ympäristön vaatimalla tavalla. Organisaatiokulttuuri on mallin mukaan yksi mukautumiskyvyn kulmakivistä. Esimerkiksi vaikutusvallan jakaminen ja kriisien hahmottamien pahaa

tahtovan tahon ja puolustajan näkökulmasta parantavat organisaation mukautumiskykyä. Myös valmiusharjoitukset, häiriösimulaatiot ja harjoittelu ylipäätään parantavat resilienssiä. (Seville ym. 2008, 83-84 ja 87)

4.2.3.6 Verkostojen resilienssimalli



Kuvio 19. Verkostojen resilienssimallissa muutosvoimat luovat haavoittuvuuksia ja hallintakeinot kyvykkyyksiä, jonka mukaan resilienssin tasapainotila määritellään.

Verkostojen resilienssimalli kuvaa organisaatioiden välillä muodostuvien tuotteiden, palveluiden, raha-asioiden ja tietovirtojen mukautumiskykyä ympäristön muutoksiin. Tutkimusten mukaan ketjumaisiin verkostoihin liittyvät riskit ovat yksi merkittävimpiä tekijöitä organisaatioiden olemassaololle, mutta niihin vaikuttavat tekijät tunnetaan keskimäärin melko huonosti. (Pettit ym. 2010, 1)

Mallia verrataan erityisesti perinteiseen riskienhallintaan ja sen riittämättömyyteen käsitellä todennäköisyyksiltään pienien ja seurauksiltaan suurien riskien hallintaa. Verkostojen resilienssimalli (kuviossa 19) kuvaa, kuinka muutosvoimat aiheuttavat **haavoittuvuuksia** ja hallintakeinot muodostavat **kyvykkyyksiä**.

Kuvan mukaan resilienssi kasvaa kyvykkyyksien lisääntyessä ja haavoittuvuuksien vähentyessä. Toisaalta kyvykkyyksien tulee kohdistua juuri oikeisiin haavoittuvuuksiin. Minkä tahansa kyvykkyyden lisääminen ei siten riitä resilienssin parantamiseksi. (Pettit ym. 2010, 4-6)

Kuviosta 19 huomataan, että liian suuri haavoittuvuuksien määrä suhteessa täsmääviin kyvykkyyksiin johtaa liialliseen riskiin. Toisaalta liialliset kyvykkyydet suhteessa haavoittuvuuksiin heikentävät organisaation toimintamahdollisuuksia ja aiheuttavat tehottomuutta. Organisaatioiden tehokkuus paranee kyvykkyyksien ja haavoittuvuuksien täsmätessä.

Mallissa listataan yleisimpiä haavoittuvuus- ja kyvykkyystekijöitä. Haavoittuvuuksia luovat esimerkiksi toimintaympäristön rauhattomuus, uhat, ulkoinen paine, resurssivajaus, herkästi häiriintyvät prosessit, organisaatioiden keskinäisriippuvuus ja alihankkijoiden ongelmat. Kyvykkyyksiä luovat hankintojen joustavuus, riittävä kapasiteetti, tehokkuus, tilannetietoisuus, palautumiskyky, ennakointi, toimintojen hajauttaminen, yhteistyö, taloudellinen vahvuus ja asioiden tehokas organisointi. (Pettit ym. 2010, 7 ja 12)

4.2.3.7 Yhdistetyn jatkuvuus -ja toipumissuunnittelun malli

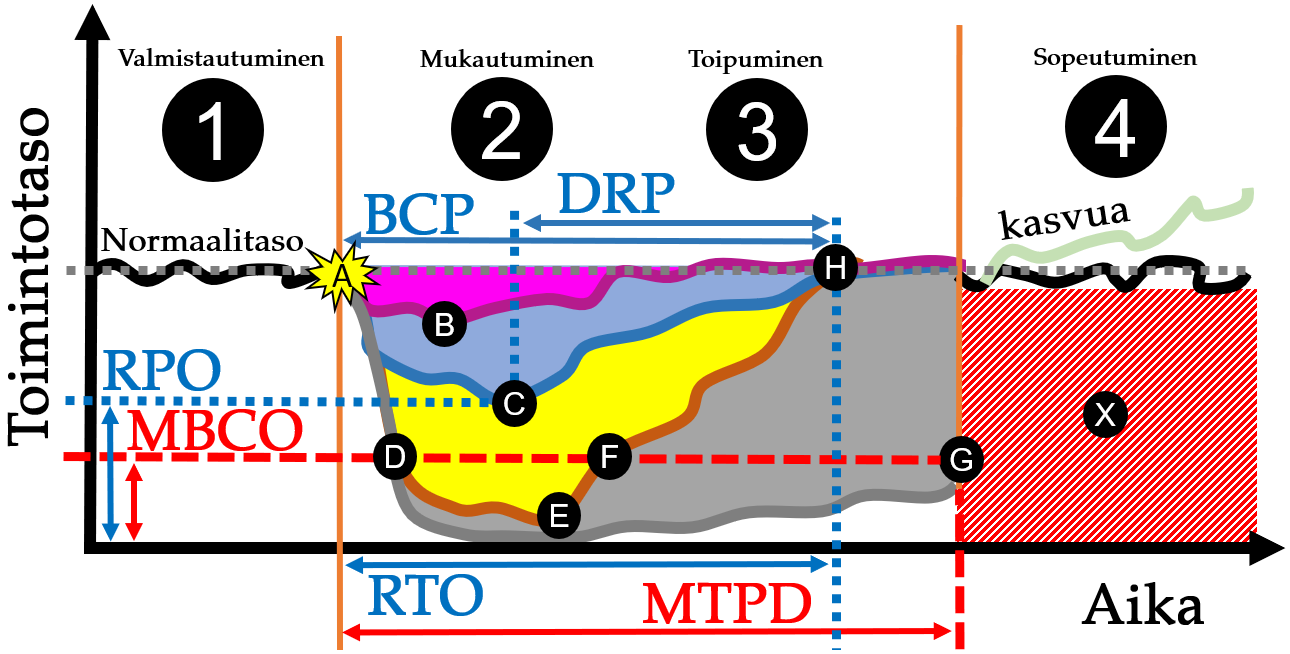
Jatkuvuus- ja toipumissuunnittelun mallin ideana on yhdistää tyypillisesti erillään pidettävät jatkuvuus- ja toipumissuunnitteluprosessit. Tällä tavoitellaan tehokkaampaa ja vaikuttavampaa elintärkeiden toimintojen keskeytyksettömyyden ja palautumisen varmistamista. Resurssien tehokkaampi ja vaikuttavampi jakaminen jatkuvuus- ja toipumissuunnitelmien välillä parantaa resilienssiä häiriötilanteessa. (Sahebjamnia ym. 2015, 261-264)

Jatkuvuussuunnittelun (engl. Business Continuity Planning, BCP) tavoitteena on suunnitella toimenpiteet elintärkeiden toimintojen säilyttämiseksi organisaation tavoitteiden kannalta hyväksyttävissä olevalla tasolla (engl. Minimum Business Continuity Objective, MBCO) kaikissa tilanteissa. Häiriöstä palautuminen tulee tapahtua etukäteen suunnitellun aikamääreen puitteissa (engl. Maximum Tolerable Period of Disruption, MTPD). Aikamääreen ylittäminen aiheuttaisi organisaation tavoitteellisen toiminnan keskeytyksen hyväksymättömissä määrin. (International Organization for Standardization 2011, 3.3 ja 3.11; Sahebjamnia ym. 2015, 261)

Toipumissuunnittelun (engl. Disaster Recovery Planning, DRP) tavoitteena on puolestaan selkeiden määriteltyjen ja dokumentoitujen toimintaohjeiden tekeminen, joilla häiriötilanteessa toimintakyky voidaan palauttaa normaalille kriisiä edeltäneelle tasolle.

Toipumissuunnitelmissa toteutunut järjestelmän toimintojen mukautumissaika (engl. Recovery Time Objective, **RTO**) kuvaa aikaa, jossa toiminnan jatkuvuuden varmistava toimintotaso todellisuudessa saavutetaan. Suurinta mahdollista järjestelmän toimintojen menetystä häiriötilanteessa kuvataan palautumistasolla (engl. Recovery Point Objective, **RPO**). Käytännössä tämä tarkoittaa esimerkiksi varmuuskopiointitiedostojen luomisen taajuutta tai varajärjestelmien ja pääjärjestelmien synkronointiväliä, joista riittävä toimintotaso voidaan häiriötilanteessa ottaa käyttöön. Tyypillisesti RPO esitetään aika-akselilla, mutta tässä

mallissa se esitetään toimintotason muutoksina. (International Organization for Standardization 2011, 3.12 ja 3.13; Sahebjamnia ym. 2015, 261 ja 263-264)



Kuvio 20. Yhdistetty jatkuvuus ja toipumissuunnittelun malli (IBCDRP) yhdistettynä Linkovin resilienssimallin vaiheisiin (numerot 1-4). Toimintotaso on ajan funktiona: pystyakselilla on toimintotaso ja vaaka-akselilla ajan kuluminen. Toimintotaso vaihtelee eri väreillä merkityissä skenaarioissa ajan kuluessa.

Kuviossa 20 pystyakselilla on esitetty vallitseva toimintotaso ja vaaka-akselilla ajan kuluminen. Violetti, sininen, ruskea ja harmaa käyrä osoittavat neljä erilaista tilanteen kehitysskenaariota. Arvot RTO, RPO, MBP ja DRP on merkitty kuvaan sinisen skenaarion mukaisesti. Jatkuvuus- ja toipumissuunnitelmat yhdistävässä käytännön toimintaan sulautettavassa mallissa (engl. Integrated Business Continuity and Disaster Recovery Planning, IBCDRP) järjestelmän resilienssi kuvataan ajan kuluessa vaihtelevalla palvelu- ja toimintotasolla (engl. operating level). Mallissa (kuvio 20) toimintojen todellisen mukautumissajan (RTO) tulee olla lyhyempi, kuin jatkuvuussuunnitelmassa määritellyn pisimmän siedettävän häiriöajan (MTPD). Vastaavasti toteutuneen palautumistason (RPO) tulee olla korkeampi, kuin toipumissuunnitelman määrittelemä alin siedettävä toimintotaso (MBCO) eli taso, jota suuremmat toimintojen menetykset ovat kestämättömiä. Esimerkiksi hyökkäys- ja keskeytyssimulaatioilla voidaan varmistaa tavoitearvojen täyttyminen. Näin voidaan parantaa organisaation mahdollisuuksia selvitä oikeista poikkeamista. Pisimmän siedettävän häiriöajan (MTPD) tai alimman siedettävän toimintotason (MBCO) ylittyessä organisaation toiminta-edellytykset lakkaavat. (Sahebjamnia ym. 2015, 261-264)

Mallissa resilienssin määrittely ja mittaaminen koostuu kahdesta arvosta: ajasta ja toimintotasosta, jotka on kuvattu kuviossa 20 vaaka- ja pystyakseleina. Kaaviossa ajan suhteen etenevällä tilanteella on neljä vaihetta vasemmalta oikealle: (1) valmistautuminen, (2) mukautuminen, (3) toipuminen ja (4) sopeutuminen.

Valmistautumisvaiheessa toimintotaso on normaalilla tasolla, kunnes huomaamatta jäänyt hallitsematon haavoittuvuus mahdollistaa uhan toteutumisen järjestelmässä pisteessä A. Tämän seurauksena järjestelmän toimintotaso laskee nopeasti. (Linkov ym. 2013, 473; Sahebjamnia ym. 2015, 261-264) Tässä vaiheessa kaaviossa esitetään esimerkinomaisesti neljä toisistaan poikkeavaa kehityskulkua eli skenaariota samalle järjestelmälle – esimerkiksi kybertilannekeskuksen asiakasorganisaatiolle.

Skenaarioita kuvaa kuviossa 20 violetti, sininen, ruskea ja harmaa käyrä, jotka kuvaavat toimintotason vaihtelua ajan kuluessa. Violetti käyrä edustaa tilannetta, jossa resursseja käytetään liikaa kyvykkyyksien ylläpitämiseksi. Tämä on kallista ja vie resursseja kasvulta ja kehitykseltä. Harmaassa skenaariossa puolestaan kyvykkyyksiä on liian vähän ja organisaation riskit toiminnan päättymisestä kasvavat erittäin suuriksi. Sinisessä ja ruskeassa skenaariossa resursseja käytetään jatkuvuuden ja toipumisen varmistamiseen violettia vähemmän ja harmaata enemmän. Sinisen ja ruskean skenaarion resurssit ovat yhtäläiset, mutta ne jaetaan jatkuvuuden ja toipumisen välillä eri tavoin. Kaikissa skenaarioissa toteutuu sama uhka saman suuruisena.

Violetissa skenaariossa järjestelmän toimintotaso laskee vain hieman suurien kyvykkyyksien ansiosta pisteessä B. Tällöin elintärkeät toiminnot eivät ole vaarassa ja palautuminenkin on nopeaa. Violetissa skenaariossa RPO-arvo on korkea ja RTO-arvo erittäin lyhyt. Tällöin resilienssi on erittäin hyvällä tasolla ja toimintotason menetys erittäin vähäistä. Näin toimittaessa suurien kyvykkyyksien jatkuva ylläpitäminen johtaa organisaation tehottomaan toimintaan ja vähentää mahdollisuuksia kasvuun ja toiminnan kehittämiseen. Tämä ei ole kestävä ratkaisu pitkällä aikavälillä monille organisaatioille. Tällainen toimintatapa voisi sopia äärimmäisen tasaista ja jatkuvaa toimintaa tarvitseville kyberavaruudessa toimiville organisaatioille, joiden ei tarvitse miettiä resurssien käyttöä. Tällaisia organisaatioita on käytännössä vähän.

Päinvastaisessa eli harmaassa skenaariossa varautumiseen eli jatkuvuus- ja toipumissuunnitteluun ei ole panostettu resursseja riittävästi. Tämä näkyy elintärkeiden toimintojen rampautumisena pitkäksi ajaksi uhan toteutuessa. Haavoittuvuuksien määrä on suuri suhteessa kyvykkyyksien määrään. Harmaassa skenaariossa pisin siedettävä häiriöaika (MTPD) ylittyy pisteessä G (RTO > MTPD) ja organisaation toimintaedellytykset lakkaavat (punaisella viivoitettu alue pisteessä X). Tämä tarkoittaa esimerkiksi konkurssia tai järjestelmän hallinnan itsenäisyyden menettämistä.

Ruskeassa skenaariossa järjestelmän toimintotaso laskee niin alhaiseksi, että organisaation toiminta tavoitteiden toteuttamiseksi keskeytyy täysin pisteessä D. Tässä skenaariossa järjestelmä ei ole hallinnassa ja elintärkeät toiminnot ovat lakanneet toimimasta hetkeksi (pisteeseen F asti). Tämä on organisaation selviytymisen tai tuhoutumisen kannalta kriittistä liian pitkään jatkuessaan. Resurssit on keskitetty ruskeassa mallissa ainoastaan toipumiseen, eikä jatkuvuussuunnittelua ole toteutettu. Ruskeassa mallissa toipuminen alkaa nopeasti pisteen E jälkeen, sillä toipumiseen on panostettu jatkuvuuden kustannuksella. Järjestelmän elintärkeät toiminnot saadaan palautettua vasta pisteessä F. (Sahebjamnia ym. 2015, 263)

Sinisessä skenaariossa järjestelmän toimintotaso laskee kuten edellisessäkin esimerkissä, kunnes jatkuvuussuunnitelman mukaiset varajärjestelyt käynnistyvät turvaamaan ja varmistamaan elintärkeiden toimintojen jatkuvuutta. Piste C esittää alimman todellisuudessa toteutuneen toimintotason (RPO), josta alkavat toipumissuunnitelman mukaiset toimenpiteet. Tässä skenaariossa järjestelmä pysyy jatkuvasti hallinnassa, sillä alimman siedettävän toimintotason raja ei alitu (MBCO). Tällainen tilanne syntyy esimerkiksi varajärjestelmien toiminnan alkaessa välittömästi. Toipuminen päästään aloittamaan nopeammin (pisteessä C), kuin ruskeassa skenaariossa (pisteessä E). (Sahebjamnia ym. 2015, 263)

Sinisessä ja ruskeassa skenaariossa resurssien käyttö on samalla tasolla, mutta toipumissuunnitelmaa (DRP) toteutettaessa huomataan, että ruskeassa skenaariossa joudutaan järjestelmien toiminta palauttamaan alhaisemmalta tasolta lähtien (piste E).

Sinisessä skenaariossa palauttaminen voidaan toteuttaa helpommin elintärkeiden toimintojen jatkuvasti toimiessa varajärjestelmien avulla (piste C). Toipuminen on ruskeassa skenaariossa sinistä nopeampaa toipumiseen panostettujen resurssien ja kyvykkyyksien ansiosta. Tästä huolimatta normaalille toimintotasolle palautumisaika on molemmissa skenaarioissa

sama pisteessä H. Tämä johtuu siitä, että molemmissa skenaarioissa on käytössä saman verran resursseja, mutta ne on jaettu toipumis- ja jatkuvuussunnitelmien välillä eri tavoin.

Tarkasteltaessa skenaariokäyrien ja normaalia toimintotasoa esittävän harmaan katkoviivan rajaamia sinistä ja keltaista aluetta huomataan, että ruskeassa skenaariossa käyrän ja normaalitasoon rajautuvan alueen pinta-ala on suurempi, kuin sinisessä skenaariossa. Pinta-alan suuruus kuvaa alentuneen resilienssin – kyvyn jatkaa toimintaa haitallisista tapahtumista huolimatta – määrää järjestelmässä. Mitä suurempi pinta-ala on, sitä enemmän resilienssiä on menetetty. Näin ollen samoilla resursseilla voidaan ylläpitää parempaa tai huonompaa resilienssitasoa. Resilienssi ei olekaan ainoastaan resurssiriippuvaista.

Tärkeää on löytää optimaalinen resurssien jakosuhde jatkuvuus ja toipumissuunnitelmien kesken niin, että järjestelmän hallinta voidaan säilyttää jatkuvasti (MBCO ei alitu) ja toipuminen on mahdollista kohtuullisessa ajassa (MTPD ei ylity) Samalla resilienssin menetystä kuvaavan pinta-alan (skenaariokäyrän ja normaalitason rajaama alue) tulisi olla mahdollisimman pieni. (Sahebjamnia ym. 2015, 262-263)

Edellä kuvatut skenaariot osoittavat, että jatkuvuus- ja toipumissuunnitelmien yhdistäminen ja resurssien jakaminen optimaalisesti niiden välillä parantaa järjestelmän resilienssiä. Kuviossa 20 havaitaan lisäksi resilienssin hallinnan vaiheet (1-4), jotka esiintyvät myös muissa resilienssitutkimuksissa, kuten Igor Linkovin tutkimusryhmän kyberjärjestelmien resilienssin mittareita käsittelevässä tutkimusraportissa. (Linkov ym. 2013, 473; Sahebjamnia ym. 2015, 261-266).

4.3 Kybertilannekeskuksen resilienssimalli

Edellä on käsitelty monia resilienssiä, tilannetietoisuutta ja kybernetiikkaa yhdisteleviä malleja, jotka eivät yksinään kykene kuvaamaan kybertilannekeskuksen vaikutuksia organisaation kyberresilienssiin. Tästä syystä edellä olevien mallien periaatteet ja tarjolla oleva tutkimustieto resilienssiin vaikuttavista tekijöistä on yhdistetty osana tutkimusprosessia ”kybertilannekeskuksen resilienssimalliksi”. Malli on esitetty graafisesti kuviossa 21.

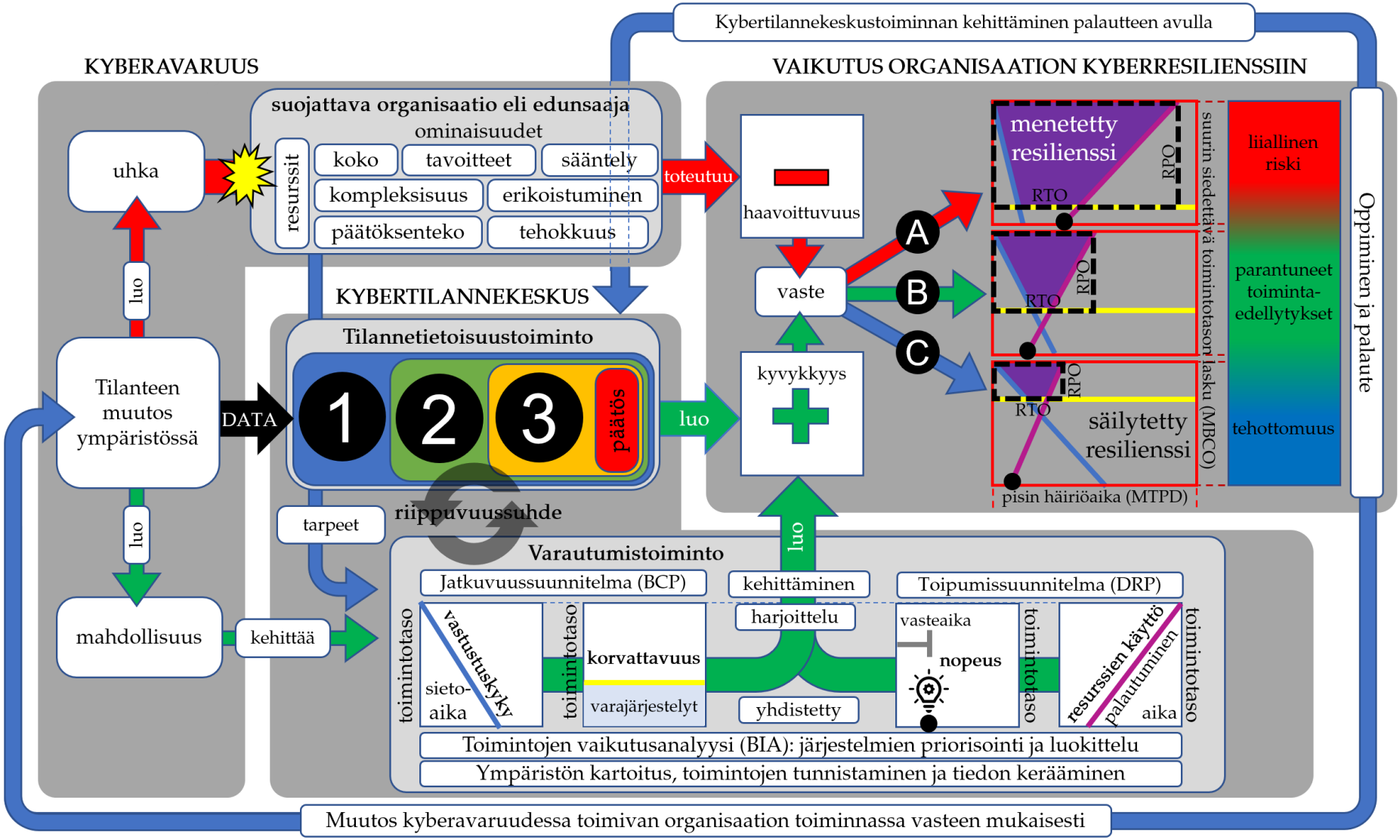
Kybertilannekeskuksen resilienssimalli kuvaa kybertilannekeskuksen toimintaa *kyberneettisenä järjestelmänä*, jonka toiminta perustuu jatkuvaan toiminnan säätelyyn palautteen pohjalta. Mallissa **ärsykkeenä** toimii kyberavaruudessa tapahtuva tilanteen muutos, joka aiheuttaa kyberavaruuteen kytkeytyneelle organisaatiolla uhan tai mahdollisuuden. Uhka

voi olla esimerkiksi muutosvoimien aikaansaaman haavoittuvuuden hyödyntäminen hyökkääjän toimesta organisaation elintärkeän tietojärjestelmän kaatamiseksi. Mahdollisuus voi olla esimerkiksi teknologia tai toimintatapa, joka mahdollistaa uuden keinon hallita haavoittuvuuksia tai luoda organisaatiolle kasvua.

Kyberavaruuden muutosvoimasta tulee uhka, jos edunsaajalla ei ole kykyä hallita muutosvoimaa. Tällöin edunsaajan kyberresilienssi on heikkoa ja epävarmuus toiminnan jatkuvuudesta kasvaa. Käytännössä lähes kaikissa järjestelmissä on haavoittuvuuksia ja ratkaisevaa onkin muutosvoimien ja hallintakeinojen yhteensovittaminen eli tasapainoinen kyberresilienssi. Kaikki hallintakeinot pohjautuvat edunsaajan näkökulmasta varautumiseen, joka muodostuu varatuista resursseista, harjoittelusta, kouluttamisesta, teknisistä valmisteluista, valmiista rakenteista, riskien arvioinnista sekä jatkuvuus- ja valmiussuunnittelusta. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 23-26)

Kuviossa 21 kybertilannekeskus **vastaanottaa** ärsykkeen aikaansaamat tilannetiedot anturoiden avulla. Tilannetietojen ja kybertilannekeskuksen kyvykkyyksien eli varautumismenettelyjen mukaisesti luodaan vallitsevasta tilanteesta tilanneymmärrys ja **päätös** tilanteen muutoksen edellyttämistä käytettävistä toimenpiteistä. Päätöksen seurauksena toteutettavat toimenpiteet **vaikuttavat** tilanteeseen. Kybertilannekeskus muodostuukin vastaanottimesta, päätöksentekoelimestä ja vaikutuselimestä. Toteutetun **vasteen** pohjalta tapahtuu kyberavaruudessa muutos, jonka toimivuutta voidaan arvioida **palautesilmukan** avulla. Palautesilmukka mahdollistaa sekä kybertilannekeskustoiminnan kehittämisen, että kybertilannekeskuksen asiakasorganisaation resilienssin jatkuvan parantamisen. Malli noudattaa kyberneettisen järjestelmän toimintaperiaatteita.

Kuviossa 21 *Organisationaalinen resilienssi- ja vastemalli* (luku 4.2.3.3) muodostaa kybertilannekeskuksen resilienssimallin rungon. Tässä tutkimuksessa havainnointiavaruus tarkoittaa kyberavaruutta. Kyberavaruus muodostaa uhkia ja mahdollisuuksia. Tilannetietoisuuden ja varautumisen muodostama kokonaisuus kuvaa kybertilannekeskuksen toimintaa, jonka onnistuminen on organisaation kyberresilienssin säilyttämisen kannalta kriittistä. Näiden kahden elementin yhteistoiminnan perusteella syntyvät toimenpiteet ovat kyvykkyyksiä, joilla vastataan haavoittuvuuden mahdollistamaan uhkaan resilientisti eli toimintakyky säilyttäen.



Kuvio 21. Kybertilannekeskuksen resilienssimalli esittää kybertilannekeskuksen vaikutuksen organisaation kyberresilienssiin. Mallissa on yhdistelty ja mukailtu monia tieteellisiä malleja: kybernetiikka (luku 4.2.3.1), organisationaalinen resilienssi- ja vastemalli (luku 4.2.3.3), tilannetietoisuuden malli (luku 4.2.3.4), resilienssin hallinnan helpotettu prosessimalli (luku 4.2.3.5), verkostojen resilienssimalli (luku 4.2.3.6) ja yhdistetyn jatkuvuus ja toipumissuunnittelun malli (luku 4.2.3.7).

Kuviossa 21 sovelletaan Endsleyn *tilannetietoisuuden mallia* (luku 4.2.3.4). Etukäteen varautumalla luodulla (1) havaitsemiskyvyllä saadaan kyberavaruudesta tilannetietoja (kuviossa musta DATA-nuoli), jotka kybertilannekeskuksessa työskentelevät ihmiset yhdistävät (2) merkitykselliseksi tilannekuvaksi etukäteen varautumalla luotujen tilannekuvaprosessien ja automaation avulla. Tämän jälkeen pyritään (3) tilanneymmärryksen luomiseen, jotta viisas ja oikea päätös ja sitä seuraavat toimenpiteet toteutuneen uhan vaikutuksien pienentämiseksi voidaan tehdä mahdollisimman nopeasti.

Kybertilannekeskuksen tilannetietoisuuden luomisen onnistuminen on riippuvainen etukäteen tehdyistä varautumistoimenpiteistä, joilla tilannetietoisuuden luominen mahdollistetaan. Varautumistoimenpiteet koostuvat järjestelmä-, ympäristö ja yksilöllisistä tekijöistä. Tästä syystä varautumis- ja tilannetietoisuustoiminta ovat kybertilannekeskuksessa täysin riippuvaisia toisistaan (kuviossa harmaa riippuvuussuhdeympyränuoli).

Kybertilannekeskuksen varautumistoiminta perustuu kybertilannekeskuksella suojattavan organisaation tarpeisiin – tavoitteisiin, tehokkaisiin toimintaperiaatteisiin, sääntelyn ja muodollisuuden asteeseen, päätöksenteon hajautuksen määrään, erikoistumiseen, kokoon ja kompleksisuuden asteeseen kybertoiminnan näkökulmasta (kuviossa ”suojattava organisaatio eli edunsaaja” -laatikko). Näitä tarpeita ja niiden vaikutusta kybertilannekeskuksen toimintaan käsitellään tarkemmin luvussa 5.4. Varautumistoiminnalla mahdollistetaan organisaation resilientti toiminta kyberavaruudessa.

Yhdistetyn jatkuvuus- ja toipumissuunnittelun mallin (luku 4.2.3.7) mukaisesti varautuminen sisältää organisaation kyberavaruuden toimintojen tunnistamisen ja toimintaympäristön kartoituksen (kuviossa ”varautumistoiminto”-laatikko). Näiden pohjalta muodostetaan toimintojen vaikutusanalyysi BIA (engl. Business Impact Analysis), jonka tarkoituksena on priorisoida ja luokitella organisaation kyberavaruuden toiminnot tärkeysjärjestykseen. Tämän jälkeen määritellään jatkuvuussuunnittelun kriteeriksi alin siedettävä toimintotaso (MBCO). Tämä tarkoittaa elintärkeitä toimintoja, jotka tulee kaikissa olosuhteissa kyetä turvaamaan, jotta organisaation toiminta on jatkuvasti hallinnassa. Toipumissuunnittelun kriteeriksi määritellään pisin siedettävä häiriöaika (MTPD). Sen ylittäminen ilman häiriön korvaamista johtaisi tuhoisiin seurauksiin organisaation kannalta, eikä siten ole hyväksyttävissä. Määritellyt MBCO- ja MTPD-arvot muodostavat ”resilienssiraamit” eli toiminta-alueen, jolla resilienssin menettäminen on mahdollista ilman organisaatiolle koituvia tuhoisia

seurauksia. Toimintotason muuttuminen ajan suhteen kuvaa tällöin organisaation kyberresilienssiä eli kykyä jatkaa haitallisista tapahtumista huolimatta. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 41-60)

Toimintojen vaikutusanalyysin (BIA) pohjalta kybertilannekeskuksessa luodaan jatkuvuus- ja toipumissuunnitelmat (BCP ja DRP) ja niiden toteuttamiseksi tarvittavat kyvykkyydet. Näiden suunnitelmien toteuttaminen yhdessä tilannetietoisuustoiminnon kanssa muodostaa organisaation kyberresilienssin tason. Suunnitelmien mukaiset toimenpiteet vaikuttavat poikkeamatilanteen kehittyessä eri ajanhetkillä. Jatkuvuussuunnitelman mukaiset toimet vaikuttavat välittömästi uhan toteutuessa kyberresilienssiä ylläpitäen. Toipumissuunnitelmalla puolestaan pyritään vastaamaan uhkaan ja aloittamaan toipuminen jälkikäteen.

Jatkuvuussuunnitelmalla (BCP) vaikutetaan organisaation kykyyn vastustaa toimintotason laskua kyberuhan toteutuessa ajan suhteen. **Vastustuskykyä** (kuvio 21) voidaan parantaa *resilienssinhallinnan helpotetun prosessimallin* (luku 4.2.3.5) mukaan ylläpitämällä korkeaa toimintotasoa uhkia varten, hallitsemalla keskeisiä haavoittuvuuksia ja tekemällä järjestelmistä häiriösietoisia tai mukautumiskykyisiä. Jatkuvuussuunnitelmalla vaikutetaan lisäksi toimintojen **korvattavuuteen** eli vaihtoehtoiseen suorittamiseen (kuvio 21). Korvattavuutta voidaan lisätä esimerkiksi korvaavien varajärjestelmien rakentamisella, vaihtoehtoisten toisistaan riippumattomien toimintatapojen kehittämisellä ja päätöksenteon hajauttamisella.

Toipumissuunnitelmalla (DRP) vaikutetaan organisaation kykyyn toipua haitallisen kybertapahtuman aikana. Toipumissuunnitemassa korostuvat tilanteenmukaisten- ja aikaisten toimenpiteiden **nopeus** ja **resurssien käyttö** viisaalla tavalla (kuvio 21). Toimenpiteiden nopeudella ja resurssien viisaalla käytöllä on suora vaikutus vasteaikaan ja häiriöajan pituuteen.

Vasteaika on tilannetietoisuusprosessissa tarvittava määrä aikaa ennen käytännön toimenpiteiden käynnistymistä. *Resilienssinhallinnan helpotetun prosessimallin* mukaan resilienssin keskeinen elementti on tilannetietoisuuden luominen oikeiden päätöksien tueksi. Mitä nopeammin tilannetiedoista muodostetaan merkityksellinen tilannekuva ja ymmärretään tilanteeseen vaikuttavia tekijöitä, sitä nopeammin voidaan tehdä viisaita ja oikeita päätöksiä uhan vaikutuksen pysäyttämiseksi ja kyberresilienssin normaalin tason palauttamisen mahdollistamiseksi. Tilannetietoisuusprosessin nopeuteen vaikuttavat havaitsemiskyky eli

tilannetietojen kattavuus, ihmisten kyky luoda merkityksellistä tilannekuvaa erilaisten järjestelmien avustuksella ja tilanneymmärrystä luovien ihmisten kokemus, koulutus ja taidot resurssien käyttämiseksi viisaalla tavalla oikeiden kyberresilienssiä parantavien päätösten tekemiseksi ja toteuttamiseksi. Toipumissuunnitelman mukaisia kyvykkyyksiä voi kehittää esimerkiksi kyberhäiriöharjoitusten muodossa.

Verkostojen resilienssimallin (luku 4.2.3.6) mukaan muutosvoimien aiheuttamien haavoittuvuuksien ja varautumalla toteutettujen hallintakeinojen eli kyvykkyyksien tulee olla järkevässä ”tasapainossa”, jotta organisaation suorituskyky tai toimintaedellytykset voivat parantua (kuviossa 21 vihreä plusmerkki ja punainen miinusmerkki). Haavoittuvuuden mahdollistaman uhan ominaisuuksia ovat esimerkiksi muutosvoiman suuruus ja haavoittuvuuden tuottama uhan kestoaika. Jatkuvuus- ja palautumissuunnitelmien mukaisesti toteutettujen kyvykkyyksien ominaisuuksia ovat puolestaan nopeus ja hallintakeinot. Haavoittuvuus ja kyvykkyydet yhdistyvät tilannevasteessa (katso ”vaste”), jonka tulos määrittelee säilytetyn ja menetetyn resilienssin suhteen pinta-alana (merkitty kuviossa 21 violetilla).

Näin saadaan selville todellisuudessa toteutunut häiriöaika RTO ja toimintotason todellinen suurin menetys RPO. Organisaation toiminnan varmistamiseksi toimintotason menetys ei saa alittaa MBCO:ta eli alinta sallittua toimintotasoa. Toisaalta toteutunut häiriöaika RTO ei saa olla pidempi, kuin pisin siedettävä häiriöaika MTPD. Mikäli RTO tai RPO ylittää edellä asetetut kriittiset arvot, organisaation toimintaedellytykset päättyvät.

Vasteen tuloksena on esitetty kolme skenaariota (kuviossa 21 (A) punainen, (B) vihreä ja (C) sininen nuoli). Skenaariot A ja C ovat tilanteita, joita tasapainoista kyberresilienssiä tavoittelevan organisaation kannattaa välttää. Tasapainoinen resilienssi tarkoittaa tilannetta, jossa resurssien käyttö ja riskien välttäminen ovat tasapainossa.

Skenaariossa A ”liiallinen riski”: haavoittuvuuden mahdollistama uhka on muutosvoimaltaan ja kestoltaan suurempi, kuin kybertilannekeskuksen tuottama kyvykkyys vastata muutosvoimaan. Esimerkiksi vastustuskyky, korvattavuus, nopeus ja resurssien tehokas käyttö ovat huonolla tasolla. Kyvykkyyksiin on käytetty resursseja riittämättömästi. Tällöin menetetyn resilienssin violetti alue on suuri ja riski kriittisten arvojen ylittämisestä kasvaa. Samalla häiriöaika on pidempi ja toimintotason lasku on muita skenaarioita suurempi.

Skenaariossa B ”parantuneet toimintaedellytykset”: kyvykkyyksien ja haavoittuvuuksien mahdollistaman uhan vaste ei aiheuta riskiä organisaation toiminnan kannalta kriittisten

arvojen ylittämisestä. Toimintaedellytykset säilyvät jatkuvasti kohtuullisella tasolla. Menetetyn resilienssin alue on pienempi, kuin skenaariossa A. Häiriöaika ja toimintotason menetys ovat skenaariota A vähäisempiä.

Skenaariossa C ”heikentynyt kannattavuus”: organisaation kyvykkyydet, kuten vastustuskyky, varajärjestelyiden määrä, vasteajan nopeus ja resurssien käyttö ovat korkealla tasolla suhteessa uhan hyödyttämään haavoittuvuuden aikaansaamaan muutosvoimaan ja kestoon. Tällöin uhan aiheuttama resilienssin menetyskin on vähäinen. Tällainen tilanne voi olla hyödyllinen organisaatioille, joille toimintatason jatkuva korkealla tasolla pitäminen on ensisijaista ja resurssit ovat suuret. Todellisuudessa moni organisaatio joutuu kuitenkin tasapainottelemaan kustannusten ja hyötyjen välimaastossa, jolloin skenaario C voi yhtä lailla muodostaa organisaation toiminnan jatkuvuudelle ongelman korkeilla kustannuksilla ja heikentyneellä kannattavuudella.

Edellä kuvattu kybertilannekeskuksen resilienssimalli selittää kybertilannekeskuksen vaikutuksia organisaation kyberresilienssiin kokonaisvaltaisesti yhdistelemällä ja soveltamalla monia tieteellisiä aiemmin julkaistuja malleja (kuvio 21). Sovellettu yhdistelmä tarjoaa kokonaiskäsityksen siitä, miten kybertilannekeskuksen varautuminen ja mahdollisuus tilanteen edellyttämään toimintaan vaikuttavat organisaation kyberresilienssiin eri skenaarioissa. Mallin mukaan keskeisiä kyberresilienssiin vaikuttavia tekijöitä ovat muutoksen vastustuskyky, toimintojen korvattavuus, toimenpiteiden nopeus ja resurssien viisas käyttö. Resilienssiin vaikuttavat lisäksi ympäristön muutosvoimien suuruus ja kesto, johon organisaatio ei voi omalla toiminnallaan juuri vaikuttaa.

Mallin mukaan kybertilannekeskuksen toiminnan onnistumisen ratkaisevat elementit ovat etukäteisvarautuminen ja tilannetietoisuuskyky. Hyvin toimivassa kybertilannekeskuksessa nämä toiminnot suunnitellaan jatkuvuus- ja toipumissuunnitelmien avulla ja toimintaa kehitetään jatkuvasti palautesilmukan avulla oppimalla. Kyvykkyyksien tulee myös vastata kyberavaruudessa toimivaan suojattavaan organisaatioon kohdistuvia uhkia ja haavoittuvuuksia tasapainoisesti – hyötyjen ja kustannusten tulee vastata suojattavan organisaation tarpeita.

5 KYBERTILANNEKESKUSTOIMINTA

Tässä luvussa tarkastellaan kybertilannekeskusta käsitteenä ja ilmiönä tarkemmin. Lisäksi määritellään kybertilannekeskuksen toiminnan keskeiset tavoitteet, tehtävät ja toimintaa ohjaavat periaatteet. Tässä luvussa on käytetty tutkimukseen kuuluneissa asiantuntijahaastatteluissa saatuja tietoja. Asiantuntijahaastatteluiden tarkemmat tiedot ja tausta on esitetty luvussa kuusi. Asiantuntijahaastatteluiden suosituksesta tässä luvussa käytetään lähteenä Carson Zimmermanin kirjoittamaa kirjaa ”Ten Strategies of a World-Class Cybersecurity Operations Center”, jota asiantuntijat kutsuivat kybertilannekeskusalan ”raamatuksi”.

5.1 Määritelmät

Kybertilannekeskus (engl. cyber security operations center, CSOC) on *organisaatio*, jossa *kyberavaruuden* muutosvoimien *havaitsemiskyvyllä* aistittavien *tilannetietojen* merkityksiä tulkitaan *tilannekuvaksi*. Se yhdistetään kokemuksen, kyvykkyyksien ja taitojen eli *varautumisen* avulla *tilanneymmärrykseksi*. Tämän perusteella päätellään ympäristön muutosvoimien aiheuttamille *haavoittuvuuksille* oikeita *tilannevasteita* eli *hallintakeinoja* edunsaajan *kyberresilienssin* parantamiseksi (kuvio 1). Kybertilannekeskuksen **tehtävä** on luoda tilannetietoisuutta ja varautumista, jotta kyberresilienssin tasoa on mahdollista säätää kyberneettisesti optimaaliselle ja tasapainoiselle tasolle riskien pienentämiseksi ja tehottomuuden välttämiseksi. Tässä luvussa käytetään tämän määritelmän osia kybertilannekeskustoiminnan tarkastelemiseksi.

Edellä kuvatun organisaation toimintaa kutsutaan **kybertilannekeskuspalveluksi**. Käytännössä se sisältää reaaliaikaisen edunsaajan eli asiakasorganisaation kyberavaruuden havainnoinnin teknisillä järjestelmillä ja mahdollisuuden ilmoituksen tekemiseen jälkikäteen jo toteutuneista poikkeamista. Tilannekeskuksen työntekijät muodostavat tilannetietojen perusteella tilannekuvaa, jota jaetaan edunsaajaorganisaatiolle sekä ulkopuolisille verkostokumppaneille hyödyllisessä muodossa. Esimerkiksi tilastoja, kuvioita ja esityksiä voidaan tarjota edunsaajaorganisaation johdon ja suunnittelun tarpeisiin. Tätä tilannekuvaa edunsaajaorganisaatio, verkostokumppanit ja kybertilannekeskus voivat käyttää varautumiseen, toiminnan kehittämiseen ja kyberresilienssin parantamiseen omien kykyjen, taitojen ja ko-

kemuksen puitteissa. Tilannevaste voi tarkoittaa esimerkiksi edunsaajaorganisaation neuvomista poikkeamasta toipumiseksi tai varsinaisen tilannevasteen toteuttamista. CSOC-palvelun laajuus ja laatu vaihtelevat asiakkaan tarpeiden mukaan. (Zimmerman 2014, 9-10)

Kybertilannekeskukselle on olemassa edellä kuvatusta poikkeavia määritelmiä, jotka korostavat esimerkiksi kyberpuolustuksellista (Zimmerman 2014, 8), liiketoiminnallista ja strategista näkökulmaa (Onwubiko 2015, 1). Jotkin määritelmät korostavat anturien tuottamien suurten datamäärien hallintaa ja analyysiä (Shah, Ganesan, Jajodia & Cam 2018, 1060). Kaikissa määritelmissä yhdistyy parempaan tilannetietoisuuteen pyrkiminen kyberavaruutta havainnoimalla.

Kybertilannekeskusorganisaatiosta käytetään vaihtelevasti erilaisia nimityksiä ja akronyymejä eli lyhenteitä eri yhteyksissä. Yleisimpiä ovat:

- SOC (Security Operations Center) eli turvallisuusoperaatiokeskus
- CSOC/ISOC (Cyber/Information Security Operations Center) eli kybertilannekeskus, kyberoperaatiokeskus, kyberturvallisuuskeskus, tietoturvavalvomo tai tietoturvahallintakeskus
- CSIRT (Computer Security Incident Response Team) eli tietoturvapoikkeamien hallintaryhmä
- CIRT (Computer/Cyber Incident Response Team) eli kyberturvallisuusryhmä
- CSIRC/CIRC (Computer Security Incident Response Center/Capability) eli kyberturvallisuuspoikkeamakeskus tai kyberkeskus.

Nimityksiä ja määritelmiä käytetään ristiriitaisesti ja päällekkäin eri yhteyksissä. (Sanastokeskus 2018; Zimmerman 2014, 8-9)

SOC-lyhenteellä voidaan kuvata myös fyysiseen – esimerkiksi toimitilaturvallisuuteen – tai muuhun tekniseen turvallisuustilannetietoisuuteen tai -tilannekuvan luomiseen erikoistuneita turvallisuusorganisaatioita, joista voidaan hallita esimerkiksi kulunvalvontaa, valaistusta, hälytyksiä, kameravalvontaa ja muuta turvallisuustekniikkaa. Tällöin ei olla kiinnostuneita suoraan kyberavaruuden, vaan sen ulkopuolelle jäävien osa-alueiden tilannetietoisuuden ja resilienssin kehittämisestä. Rajanveto ja eron kuvaaminen SOC-toiminnan ja aiemmin kuvatun – tässä tutkimuksessa kiinnostuksen kohteena olevan – CSOC palvelun välillä on tällä tavalla melko helppoa, mutta ei välttämättä hedelmällistä kyberavaruuden

ja sen fyysisen vaikutusalueen jatkuvasti kasvavan kytkeytymisen takia. Esimerkiksi esineiden internetin (engl. IoT, Internet of Things) kehittyessä on mahdollista, että edellä mainittujen palveluiden yhdistäminen toisi synergiaetuja turvallisuusnäkökulmasta. Esimerkiksi muodostettaessa tilanneymmärrystä voivat kulun- tai videovalvontatiedot olla hyödyllisiä kokonaiskäsityksen aikaansaamiseksi. Vastaavasti esimerkiksi teollisuusautomaatiojärjestelmään jo toteutuneen kyberuhkan tapahtumien kokonaiskuvan ja vaikutuksien ymmärtämisessä voi olla hyötyä vastaavista tiedoista. (Nadel 2004, 2.20)

5.2 Organisaationäkökulma kybertilannekeskukseen

Organisaatio – kuten kybertilannekeskus – voidaan määritellä neljästä eri näkökulmasta:

- rationaalisesta (engl. rational system)
- luonnollisesta (engl. natural system)
- avoimesta (engl. open system)
- kulttuurillisesta (engl. cultural system).

Valinta vaikuttaa kybertilannekeskuksen tutkimiseen, kehittämiseen ja mieltämiseen oleellisesti. (Harisalo 2008, 17-19; Scott & Davis 2015, 35-106)

Rationaalisesta – tavoitteiden ja tehtävien tehokkaan saavuttamisen – näkökulmasta kybertilannekeskuksella pyritään kyberturvallisuustasoa eli kyberresilienssiä nostamalla saavuttamaan enemmän taloudellista hyötyä suhteessa rahalliseen – kyberuhkien mahdollisesta toteutumisesta aiheutuvaan menetykseen. Tällainen näkökulma on tyypillinen esimerkiksi yksityisellä ja julkisella sektorilla toimiville yhtiöille, joiden tehtävänä on toimia tehokkaasti voiton tuottamiseksi omistajilleen. (Harisalo 2008, 17-19)

Luonnollisesta – jatkuvuuden ja olemassaolon turvaamisen – näkökulmasta kybertilannekeskuksella mahdollistetaan edunsaajaorganisaation olemassaolo, selviytyminen ja säilyminen. Ainoastaan tehokkuuteen ja tavoitteellisuuteen keskittyminen vaarantaisi edunsaajaorganisaation olemassaolon. Tämän näkökulman mukaan kybertilannekeskuksella ei haeta ensisijaisesti tehtävien tehokkuutta, vaan sen avulla ylipäätään mahdollistetaan toiminta kyberavaruudessa. (Scott & Davis 2015, 60 ja 61) Eräs esimerkki tällaisesta edunsaajaorganisaatiosta on valtiollinen toimija, joka haluaa seurata kyberavaruuden käyttäjien toimia esi-

merkiksi kansallisen turvallisuuden nimissä. Tällöin valtiollinen toimija, kuten puolue, näkee kyberavaruuden käyttäjät potentiaalisina uhkina olemassaololleen ja toiminnan jatkuvuudelle. Tästä esimerkkinä Kiinan harjoittama politiikka ja kyberturvallisuuslaki, joka rajoittaa kyberavaruuden käyttäjien anonymiteettiä ja velvoittaa yritykset raportoimaan poikkeavuuksista valtiolle. Samantapaista valvonnan kiristämisen kehitystä ja internetin pirstaloitumista on havaittavissa myös esimerkiksi Venäjällä, Vietnamissa, Tansaniassa, Nigeriassa, Etiopiassa, Sudanissa ja Egyptissä. Kybertilannekeskuksia voidaankin käyttää myös tästä näkökulmasta muutosvoimien hallinnan välineenä. (Harisalo 2008, 17-19; Lyytikkä & Hallamaa 2018)

Avoimesta eli ympäristön vuorovaikutuksen ja havaintojen avulla kehittymisen sekä ympäristön tarpeiden tyydyttämisen näkökulmasta kybertilannekeskuksella tarkkaillaan toimintaympäristöä, kehitetään toimintaa havaintojen perusteella ja tyydytetään ympäristön vaatimuksia. Tästä avoimen järjestelmän näkökulmasta kybertilannekeskus tuottaa tietämystä ympäristön olosuhteista, jotka rajoittavat ja suuntaavat edunsaajaorganisaation mahdollisuuksia kehittyä. Menestyvä edunsaajaorganisaatio toimii havainnoimalla kyberavaruuden muutosvoimia, muuttaa toimintaansa varautumalla eli luomalla kyvykkyyksiä havaintojen pohjalta sekä tyydyttää ympäristön eli kumppanien, verkostojen ja strategisten sopimusosapuolien vaatimukset. Näihin tarpeisiin kybertilannekeskus tyypillisesti vastaa. Tällaisen edunsaajaorganisaation toiminta on riippuvainen verkostoista ja vuorovaikutuksesta toimintaympäristön kanssa ja prosessien kehittäminen on rakenteiden kehittämistä tärkeämmässä roolissa. (Harisalo 2008, 17-19)

Kulttuurillisesta – tulkintojen, käsitysten ja mielikuvien – näkökulmasta kybertilannekeskus nähdään kulttuurillisena mallina tarkoitusten ja merkityksien kautta. Ihmisten kanssakäyminen ja kanssakäymistä lisäävät tekijät ovat tästä näkökulmasta kybertilannekeskukselle tärkeitä voimavaroja. Esimerkiksi työntekijöiden erilaiset roolit, työtehtävät ja keskinäinen yhteistyö määrittävät tässä näkökulmassa kybertilannekeskuksen olemuksen. (Harisalo 2008, 17-19)

Tässä tutkimuksessa kybertilannekeskus nähdään ensisijaisesti edellä esitetyn kolmannen näkökulman mukaan *avoimeksi* järjestelmäksi, joka kuvaa hyvin kybertilannekeskuksen empiiristä toimintaa ympäristön vuorovaikutuksen, havainnoilla kehittymisen ja ympäristön vaatimuksien täyttämisestä johtuen. Teoriatausta kybertilannekeskuksen toiminnasta tukee

hyvin toimintaympäristöä korostavaa roolia. Organisaationa kybertilannekeskuksen ensisijainen tavoite onkin ympäristön vaatimuksien täyttäminen. Seuraavaksi tarkastellaan ympäristön asettamia vaatimuksia, resursseja ja toimivaltuuksia kybertilannekeskuksen ja edunsaajaorganisaation suhteena.

5.3 Suhde edunsaajaan, resurssijako ja toimivaltuudet

Edunsaaja (engl. constituency) eli asiakasorganisaatio on taho, jolle kybertilannekeskus tarjoaa palveluita. Edunsaaja on tyypillisesti kyberavaruutta käyttäviä henkilöitä, laitteita, dataa ja verkkoja ylläpitävä organisaatio. Edunsaaja voi rajautua organisatorisesti (esimerkiksi yhtiö, virasto), maantieteellisesti (esimerkiksi valtio, aluehallintoviranomainen), poliittisesti (esimerkiksi puolue, aktivistiyhteisö), teknisesti (esimerkiksi verkkosivusto, palvelin ja tietoliikenneyhteys) tai sopimuspohjaisesti (esimerkiksi internetin nimipalvelujärjestelmä, standardit ja toimintatavat). (Zimmerman 2014, 9) Kybertilannekeskuksen toimintamallia tarkastellaan kolmesta näkökulmasta: suhde edunsaajaan, resurssien jakautuminen ja toimivaltuudet. (Zimmerman 2014, 15)

Kybertilannekeskus (organisaatio A) voi olla osa edunsaajaa (organisaatio B) tai siitä erillinen. Ensimmäisessä toimintamallissa kybertilannekeskus on osa linjaorganisaatiota, kuten yritystä, yliopistoa tai virastoa. Tällöin suhde edunsaajaan on *sisäinen*. Toisessa toimintamallissa kybertilannekeskus on täysin erillinen oma organisaationsa, joka tuottaa kybertilannekeskuspalvelua hallittuna turvallisuuspalveluiden tarjoajana (engl. Managed Security Service Provider, MSSP) maksua tai muuta hyötyä vastaan. Tällöin suhde edunsaajaan on *ulkoinen*. (Zimmerman 2014, 15)

Edunsaajaorganisaatio voi valita toimintamallin tarpeidensa mukaisesti: (1) kybertilannekeskuspalvelua ei tarvita – toimitaan täysin ilman, palvelu tuotetaan (2) sisäisesti, (3) ulkoisesti tai (4) hybridimallilla. (Zimmerman 2014, 15) Hybridimallissa on kyse toiminnasta, jossa kybertilannekeskuspalvelusta osa tuotetaan *sisäisesti* ja osa *ulkoisesti*. Esimerkiksi perustoiminnot voidaan suorittaa organisaation sisäisesti ja vaativampi asiantuntija-apu hankkia ulkoisesti tai päinvastoin.

Edellä olevan jaottelun lisäksi kybertilannekeskuksen toimintamalli voidaan jaotella **resurssien** jakautumisen mukaisesti: (1) kyberturvallisuusryhmä (2) hajautettu (3) keskitetty (4)

porrastettu tai (5) koordinoiva. *Kyberturvallisuusryhmä* on tarpeen tullen organisaation työntekijöistä koostettava väliaikainen organisaatio, joka selvittää jälkikäteen jo toteutuneita uhkia ja lopettaa toimintansa tilanteen normalisoiduttua. Kyberturvallisuusryhmä ei täytä tässä tutkimuksessa kybertilannekeskuksen kriteereitä (katso kybertilannekeskuksen määritelmä). *Hajautetussa* mallissa kybertilannekeskus koostuu työntekijöistä, joiden pääasiallinen työtehtävä ei ole kybertilannekeskustoiminta, vaan sitä tuotetaan jatkuvana palveluna oman toimen ohella. *Keskitetty* malli koostuu kybertilannekeskuksessa toimivasta asiantuntijaryhmästä, jonka työnä on tuottaa jatkuvaa kybertilannekeskuspalvelua itsenäisenä organisaationaan. *Porrastetussa* mallissa keskitetty kybertilannekeskusryhmä tuottaa suurimman osan jatkuvista kybertilannekeskuspalveluista ja saa tarvittaessa asiantuntijaresursseja käyttöön muilta organisaatioilta. *Koordinoivassa* mallissa yksi johto-organisaatio koordinoi tai tukee montaa toisistaan erillistä kybertilannekeskusorganisaatiota ja tarjoaa erityisasiantuntijuutta vaativia palveluita sekä tekee tutkimustoimintaa. Koordinoiva keskus saa tilannetietoa tyypillisesti enemmän verkostolähtöisesti, kuin kyberavaruutta suoraan havainnoimalla. (Zimmerman 2014, 15-17 ja 51-53)

Kybertilannekeskusorganisaation **toimivaltuudet** voidaan jakaa kahteen tarkasteltavaan osaan (1) havainnointikyvykkyyden laajuuteen ja (2) tilannevasteissa käytettävään harkinnan määrään. (Zimmerman 2014, 17-18)

Ensimmäinen eli *havainnointikyvykkyyden laajuus* kuvaa, kuinka laajaan edunsaajan kyberavaruuden osaan kybertilannekeskuksella on havainnointioikeus. Edunsaaja on voinut esimerkiksi määritellä järjestelmiä, joihin kybertilannekeskuksellakaan ei ole pääsyä. Toisaalta havainnointikykyä eli tilannetietoisuuden muodostamista ei tyypillisesti kannata rajoittaa ilman erityisen painavaa perustetta, sillä näin toimittaessa ei ole mahdollista muodostaa tilannetietoisuutta. (Zimmerman 2014, 17-18)

Toinen kuvaa *harkinnan määrää*, jota organisaatio voi käyttää *tilannevasteiden osalta* suhteessa edunsaajaan. Toimivaltuudet eivät voi ylittää edunsaajan lainsäädännöllä asetettuja toimivaltuuksia. Tämä tarkoittaa, että palvelua tilaava organisaatio voi luovuttaa enimmillään vain kaikki omat toimivaltuutensa kybertilannekeskukselle. Tilannevasteiden toimivaltuudet suhteessa edunsaajaan voidaan jaotella vielä lisäksi esimerkiksi seuraavasti: (1) ei toimivaltuutta, (2) jaettu toimivaltuus tai (3) täysi toimivaltuus.

Ensimmäisessä tapauksessa kybertilannekeskus toimii neuvonantajan ja tilannekuvan tuottajan roolissa. Tällöin tilannevasteet ovat suosituksia edunsaajalle, joka päättää itsenäisesti toteuttaako kybertilannekeskus vasteen vai ei. Toisessa tapauksessa edunsaajan edustajat ja kybertilannekeskus muodostavat johtoryhmän tai muun yhteistyöelimen, jossa jokaisella on tietty ennalta määrätty valta päättää kannastaan ja tasatilanteessa äänestää suositellun vasteen toteuttamisesta. Kolmannessa tapauksessa kybertilannekeskuksella on täysi toimivaltuus määrätä tilannevasteita edunsaajaorganisaation kyberresilienssin parantamisen ja varmistamisen osalta. Tässä tapauksessa keskuksella on suora pääsy edunsaajan kyberavaruuden piirissä oleviin järjestelmiin tai keskus voi edellyttää edunsaajaorganisaation tekemään muutoksia kyberresilienssin parantamiseksi. (Zimmerman 2014, 17-18)

Edunsaajaorganisaation myöntäessä toimivaltuuksia, se aina siirtää osan vallastaan ja hallinnastaan kybertilannekeskukselle. Toisaalta vähäiset toimivaltuudet omaava kybertilannekeskus on hidas (reagoiva) ja kankea (ennaltaehkäisyä painottava), sillä päätöksen tekemisessä kuluu huomattavasti aikaa. Täydet toimivaltuudet hyödyttäisivät kyberresilienssin kehittämisessä parhaiten, mutta tällöin kyberavaruuden hallinta menetettäisiin kybertilannekeskuspalveluntarjoajalle. Toimivaltuusasiassa edunsaajan onkin tasapainoiltava aikakriittisyyden ja palveluntuottajalle luottamuksen välillä.

5.4 Toimintamallin valinta edunsaajan tarpeiden mukaisesti

Edellä kuvattujen toimintamallien valinta tulisi aina perustua edunsaajaorganisaation tarpeisiin ja ominaisuuksiin kyberavaruuteen nähden, kuten: *tavoitteisiin*, *rationaalisuuteen* eli valittujen keinojen tehokkuuteen, *muodollisuuden* eli lainsäädännön tai sisäisen sääntelyn *määrään*, *keskittämisen* ja *hajauttamisen* määrään, toimialakohtaisen *erikoistumisen* tasoon, organisaation *kokoon* ja käsiteltävien asioiden *kompleksisuuteen*. (Harisalo 2008, 19-28; Zimmerman 2014, 50) Lisäksi edunsaajan tarpeisiin vaikuttavat kyberavaruuden muutosvoimat eli vallitsevat uhat.

Toimintamallin valintaan vaikuttaa edunsaajan **tavoite** eli olemassaolon tarkoitus. Käytännössä tällä tarkoitetaan organisaation kyberavaruudessa toimimisen kannalta *arvokkaiden* ja *arvoa luovien* asioiden tunnistamista ja niiden suojaamista (ICANN 2015). Esimerkiksi julkisorganisaatiot toimivat toimeksiantotalouden pohjalta ja tavoittelevat mahdollisimman

suurta julkista arvoa politiisen, taloudellisen, sosiaalisen ja kulttuurillisen toiminnan edistämiseksi. Tällöin tavoitteena on näiden toiminta-alueiden tukemiseksi auttaa toimijoita sopeutumaan kyberavaruuden muutosvoimiin ja näin varmistaa yhteiskunnan sekä kansalaisten etujen toteutuminen kyberavaruudessa viimekädessä vallankäytöllä. (Benington & Moore 2011, 3-4; Garofalo 2015, 191) Tällöin luonnolliseksi toimintamallin valinnaksi tulisi sisäinen, täysin toimivaltainen, koordinoiva kybertilannekeskuspalvelu, jonka tavoitteena olisi tarjota palveluita ja luoda verkostoja kyberavaruudessa toimivien tahojen välille kybertilannetietoisuuden ja kyberturvallisuuden kehittämiseksi sekä varmistaa lain noudattaminen pitämällä yllä omaa tilannekuvaa. Näin toimii Suomessa esimerkiksi Traficomin Kyberturvallisuuskeskus, joka tuottaa kyberturvallisuuden tilannekuvaa, muodostaa tutkimustietoa erilaisista trendeistä ja toimii valvovassa sekä koordinoivassa viranomaistehtävässä yhteistyössä yksityisen ja julkisen sektorin muiden toimijoiden kanssa. (Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen 2018, 23, 30-31, 33, 38 ja 46)

Edunsaajan näkökulmasta on tärkeää toimia **rationaalisesti** eli käyttämällä tehokkaimpia menetelmiä tavoitteen saavuttamiseksi. Tavoitteena voivat olla esimerkiksi pienentää toteutuneista kyberuhkista aiheutuneita menoja, vähentää toiminnan riskejä, lisätä asiakastyytyväisyyttä, lisätä työntekijöiden tyytyväisyyttä tai täyttää viranomaisvaatimuksia (Dalziel 2014, 7-8). Toisaalta, ainoastaan rationaalisesti toimien ei voida keksiä uusia asioita ja ratkaisuja kyberavaruuden ongelmiin. (Harisalo 2008, 21-22) Tällöin ulkoinen, keskitetty ja täydet toimivaltuudet omaava luotettu kybertilannekeskuspalveluntarjoaja voi olla toimintamalliksi parempi valinta kustannustehokkuusmielessä, mutta sisäinen omista työntekijöistä koostuva ratkaisu voi olla innovaatiomielessä tehokkaampi ja tukea myös organisaation kehittymistä, arvoja ja resilienttiä toimintaa paremmin. Edunsaaja voi esimerkiksi strategisella valinnalla profiloitua kyberavaruuden toiminnasta riippuvaiseksi tahoksi, joka haluaa itse tuottaa kybertilannekeskuspalvelun ja taata asiakkailleen kybertoiminnan turvallisuuden.

Muodollisuus eli edunsaajaan kohdistuvan sääntelyn määrä vaikuttaa toimivaltuussuhteen valintaan. Esimerkiksi kybertoiminnan laatua, ennustettavuutta ja tuottavuutta tavoitteleva edunsaaja ohjaa erilaisilla ohjeilla ja määräyksillä toimintaansa. Vaatimuksena voi olla vaikkapa kyberturvallisuuden hallintajärjestelmän mukainen tilannevaste tietyn kyberuhkan toteutuessa. Tällöin kybertilannekeskus voisi toimia edunsaajaorganisaation johdon

alaisuudessa ilman toimivaltuutta tai jaetulla toimivaltuudella. Kääntöpuolena on aikaviiveen ja jäykkyyden lisääntyminen. (Harisalo 2008, 22-23; Zimmerman 2014, 50)

Edunsaajaorganisaatio saattaa haluta myös **keskittää** tai **hajauttaa** kyberasioihin liittyvää päätösvaltaa ja toimivaltuuksia tilanteesta riippuen. Keskittäminen on tyypillisesti järkevää jo toteutuneista kriiseistä ja uhkista selviytymiseksi. Tällöin ylimmällä johdolla on paras mahdollisuus hallita toimintaa, mutta virheellisten ratkaisuiden todennäköisyys kasvaa. Hajauttaminen puolestaan voi olla järkevää muutosvoimien ja epävarmuuden lisääntyessä, mutta tällöin edunsaajaorganisaation johdon valta päättää asioista heikkenee. Hajauttaminen tyypillisesti johtaa korkeampaan tiedonvälityksen, sitoutumisen ja työtyytyväisyyden tasoon. Esimerkiksi edunsaajan tietoteknisten palveluiden hankinta on tyypillisesti ulkoistettu, jolloin kybertilannekeskuspalveluiden hankinnasta eri toimijalta voi olla hajautusmielessä etuja. Samalla ulkopuolinen taho valvoo ulkoistettua kyberavaruuden toimintaa, jolla palvelun laatutaso voidaan varmentaa. (Harisalo 2008, 23-24)

Myös edunsaajaorganisaation **erikoistuminen** eli toimiala ja sisäinen järjestäytyminen eri osastoihin vaikuttavat kybertilannekeskuksen toimintamallin valintaan. Esimerkiksi tietotekniikka-alalla toimivalla edunsaajalla saattaa olla henkilöstössään kybertilannekeskuksien tarvitsemaa osaamista. Tällöin porrastettu malli, jossa edunsaajaorganisaation omia toiminnan valmiiksi tuntevia asiantuntijoita käytetään tarvittaessa voi olla erittäin hyödyllinen synergiaedun näkökulmasta. Esimerkiksi monien automaatiojärjestelmien osalta kybertilannekuvan luominen ei ole mahdollista ilman alakohtaista erikoisosaamista, jolloin tarjontaa ulkoisesti tuotetulle kybertilannekeskuspalvelulle voi olla haastavaa löytää. Tietotekniikka-alan organisaatioon verrattuna päinvastaisessa tilanteessa edunsaajan liiketoiminta ei ole millään tavoin riippuvainen kyberavaruudesta tai toimi sen kautta, jolloin kybertilannekeskuspalveluille ei ole välttämättä tarvetta lainkaan. Hyvin harva organisaatio voi nykyään kuitenkaan toimia riippumatta tietotekniikasta ja kyberavaruudesta, sillä esimerkiksi maksuliikenne, työn tekeminen ja osa infrastruktuurin ohjaamisesta tapahtuu nykyään kyberavaruudessa. (Harisalo 2008, 24-25)

Edunsaajaorganisaation **koko** tarkoittaa kybertilannekeskuksen näkökulmasta kyberavaruuteen kytkeytymisen osuutta käyttäjien, IP-osoitteiden ja laitteiden määrällä mitattuna. Mitä suurempi edunsaajan koko kyberavaruudessa on, sitä suurempi tarvittava kybertilan-

nekeskusorganisaatio tyypillisesti on. (Zimmerman 2014, 50) Muita edunsaajan koon määrittäviä asioita ovat esimerkiksi henkilöstömäärä tai liikevaihto (Harisalo 2008, 25-27). Nämä vaikuttavat kybertilannekeskuksen toimintamallin valintaan, sillä kybertilannekeskuspalvelun tuottaminen sisäisesti vaatii tarpeeksi suuria resursseja – osaavaa henkilöstöä, verkostokumppaneita ja pääomaa – joita esimerkiksi pienillä ja keskisuurilla yrityksillä harvoin on. Tällöin ulkoisesti hankittu palvelu voi olla oikea keino päästä tavoitteeseen.

Viimeinen toimintamallin valintaan vaikuttava edunsaajan osa-alue on toiminnan **kompleksisuus**. Esimerkiksi konglomeraatti eli monialayhtiö tai valtion- ja kunnallishallinto voivat toimia hyvinkin eri tavoin toimialoittain ja niillä voi olla merkittävä määrä kyberavaruuden keskinäisriippuvuuksia, joita on vaikea tunnistaa. Käytännössä tämä tarkoittaa, että kyberavaruudessa toimivat järjestelmät ovat pirstaleisia ja monien rajapintojen takia yhteydessä toisiinsa, jolloin harva tuntee täysin järjestelmien vaikutuksia toisiinsa. Tällöin kybertilannekeskuspalvelun toimintamallissa tulee ottaa huomioon alakohtaiset tarpeet, niiden toteuttaminen ja tunnistaa tilanneymmärryksen luomiseen liittyvät haasteet. Esimerkiksi koordinoiva kybertilannekeskus alikeskuksineen tai porrastettu malli alakohtaisine asiantuntijoineen voisi olla toimiva ratkaisu. (Harisalo 2008, 25-27)

Toisin kuin (Zimmerman 2014, 50) väittää, tämän tutkimuksen havaintojen perusteella ei ole järkevää valita kybertilannekeskuksen toimintamallia havaittujen kyberhäiriöiden lukumäärän perusteella, sillä kuten johdannossakin kuvailtiin, suuri osa toteutuneista kyberuhkista jää havaitsematta tai havaitaan jälkikäteen. Tällöin kyberresilienssin taso eli kyvykkyyksien ja haavoittuvuuksien suhde on väärin mitoitettu.

Yhtä kaikki, kybertilannekeskuksen toimintamalli voi olla hyvin monenlainen ja valitun ratkaisun eli keinojen tulisi pohjautua edunsaajaorganisaation tarpeisiin. Tilannetta, jossa keinoista (kybertilannekeskuspalvelu) tulee tarve ja tarpeista (kyberresilienssi) keino kannattaa välttää (Harisalo 2008, 20). Näin voi käydä tilanteessa, jossa kybertilannekeskuspalvelun tuottajan tavoitteeksi tulee kyberresilienssin ja tilannetietoisuuden parantamisen sijasta kybertilannekeskuksen ylläpitäminen ja olemassaolon varmistaminen.

Toisaalta on huomioitava, että kyberresilienssin tarpeen määrittäminen on erittäin haasteellista ilman kybertilannekeskuksen tarjoamaa tilannekuvaa kyberavaruudesta. Toisin, kuin Zimmerman kirjassaan väittää (Zimmerman 2014, 50), erilaisten kyberturvallisuusongel-

mien poissaolo ei välttämättä tarkoita kyberresilienssin tarpeen vähenemistä tai vähäisyyttä, vaan voi tarkoittaa esimerkiksi huonoa tilannetietoisuutta. Tästä syystä edunsaajan on kaikissa tapauksissa hyvä olla tilannetietoinen siitä, mitä omaa organisaatiota koskettavassa kyberavaruudessa tapahtuu, sillä vain siten voidaan määrittää kyberresilienssin tarve ja oikeat keinot eli kybertilannekeskuksen haluttu toimintamalli.

5.5 Kyberaistien eli anturien ominaisuudet

Tehtävänsä täyttämiseksi kybertilannekeskuksen on havaittava edunsaajaorganisaatioon kohdistuvat kyberavaruuden muutosvoimat. Kaikki kyberavaruuden muutosvoimat ovat symbolisia eli biteillä 0 tai 1 muodostettuja eroavaisuuksia. Ihminen ei voi aisteillaan suoraan havaita kyberavaruuden muutoksia. Tällöin niiden havainnointiin tarvitaan edunsaajan tietotekniseen ympäristöön kytkettäviä kyberantureita eli datan välittäjiä, agentteja tai aisteja (Luciano & Zalta 2019).

Kyberanturit muodostava yhdessä aistitason, joka määrittelee havaitsemiskyvyn kattavuuden. Kyberanturit toimivat kuten fyysisen maailman tapahtumien ja muutoksien havaitsemiseen erikoistuneet elektroniset anturit, mutta aistivat kyberavaruudessa liikkuvien bittien eroavaisuuksia. Esimerkiksi kyberanturit, paikkatietoanturit, liiketunnistimet ja lämpöanturit välittävät kyberavaruuden ja fyysisen maailman muutokset eli tosiot tietoliikenneyhteyksien avulla bitteinä haluttuun keskitettyyn paikkaan kybertilannekeskuksessa lähes viiveettä. (Berger, Hees, Braunreuther & Reinhart 2016, 638-640)

Kuten ihmisen silmällä, korvalla ja nenällä aistieliminä on tietty rakenne ja ominaisuudet, myös kyberaisteilla on ominaisuuksia. Kaikkia kyberantureita eli kyberavaruuden aisteja voidaan tarkastella seuraavassa sovelletun ja kyberavaruuden periaatteisiin muutetun yleisen *anturimallin* avulla, jossa antureiden ominaisuudet koostuvat seitsemästä ominaisuustasosta (taulukko 1) (Dasgupta, Chattopadhyay, Pal & Chakravarty 2014, 68-70).

Anturimallissa *toimintaympäristö* (taso 1) kertoo kyberavaruuden muutoksia seuraavan kyberanturin fyysisen ja tietoteknisen toimintaympäristön tunnusmerkit. Fyysisiä tunnusmerkkejä ovat esimerkiksi sisä- tai ulkotila, häiriötekijät, eristetty tila ja laitteiston sähkönsaanti. Tietoteknisiä tunnusmerkkejä ovat esimerkiksi tietoliikenteen määrä ja laatu – kuten salaus – verkon muutokset ja aikakriittisyys. Toimintaympäristö vaikuttaa laiteantureiden

osalta datansaannin jatkuvuuteen, antureiden huoltoon ja elinkaareen, joka on tärkeä tunnistaa antureiden sijoittelua ja toimintaa suunniteltaessa. (Dasgupta ym. 2014, 68-69) Tyypillisesti kyberanturin on oltava fyysisesti lähellä seurattavaa kohdetta (Zimmerman 2014, 209). Lisäksi monet anturialustat ovat sijainniltaan liikkuvia niin kyberavaruuden, kuin fyysisenkin paikan osalta. Esimerkkeinä älypuhelimet ja erilaiset esineiden internetin laitteet.

Taso	Kuvaus	Aistielin: ihmisen silmä	Aistielin: kyberanturi
7	Tulkittavuus	Aivokuorelle lähetetään valoärsykesignaaleja, joissa paikan ja suunnan merkitys vaihtelee.	Data lähetetään standardinmukaisessa formaatissa, kuten syslog-muotoisena ja ymmärrettävänä.
6	Toimintaohjeet	Gangliosolut siirtävät näköaistimuksen aivoihin sähkökemiallisina ”on” ja ”off” -vastesignaaleilla.	Datalähetys suoritetaan erillisellä salatulla ja varmennetulla tietoliikenneyhteydellä asetettuun osoitteeseen.
5	Toiminnallisuus	Passiivinen vastaanottava havaitsemiskyky.	Passiivinen tai aktiivinen havaitsemiskyky.
4	Toimintatapa	Verkkokalvolla valoenergia eli fotonit muuttuvat impulsseiksi.	Siirtotiellä olevat eroavaisuudet muutetaan johtokoodin avulla symboleiksi (biteiksi).
3	Sijainti	Pääkallon silmäkuoppa, katvealue taakse 180 astetta pään ja silmän asennon mukaisesti.	Organisaation internet-liikenteen yhdyskäytävä (sisään ja ulos menevä liikenne). Katvealue sisäverkon toimintaan.
2	Ulkoinen kuvaus	Erillinen pallomainen aistielin, 25 mm halkaisija.	Erillinen anturilaite, ohjelmisto tai lokittava palvelu.
1	Toimintaympäristö	Kylmyys, kuumuus, kuivuus, vaihteleva ilmanpaine ja valon määrä. Tarkan näkemisen alueen datakapasiteetti noin 600 000 bittiä sekunnissa.	Ilmastoitu lukittu palvelintila, varavirtavarmennus. Havaittavan datan maksimimäärä esimerkiksi 10 gigabitti sekunnissa.

Taulukko 1. Taulukossa kuvataan muokattu yleinen anturimalli (Dasgupta ym. 2014, 69). Sarakkeista löytyvät tason numero, kuvaus ja kahden ”aistielimen” ominaisuuksien vertailu tasoittain. Esimerkkeinä ihmisen silmä ja kyberanturi. (Acharya, Ng & Suri 2008, 1-9, BioMag Laboratory 2016)

Anturin *ulkoinen kuvaus* (taso 2) määrittelee, millaisesta kyberanturista on kyse (Dasgupta ym. 2014, 69). Kyberanturit voidaan jakaa (1) erillisiin anturilaitteisiin ohjelmistoineen ja (2) erillisiin ohjelmistoihin, jotka asennetaan aistimaan jonkin laitteen toimintaa ja (3) palveluihin ja laitteisiin, jotka tuottavat omasta toiminnastaan dataa eli lokitietoa. Esimerkiksi ohjelmistoanturit ovat riippuvaisia laitteesta tai palvelusta, johon ne on asennettu.

Anturin *sijainti* (taso 3) suhteessa edunsaajan muihin kyberavaruuden järjestelmiin määrittelee anturin tuottaman datan lähteen paikan. Tyypillisesti edunsaajan kyberavaruuteen

tarvitaan useita antureita eli aisteja, joiden oikea sijoittelu on tärkeää mahdollisimman laajan havaitsemiskyvyn saavuttamiseksi ja katvealueiden välttämiseksi. Kyberavaruuden muutosvoimien havaitsemiskyvyn laajuus on vain kybertilannekeskukselle kuuluvaa tietoa, jonka paljastuminen ulkopuolisille voi luoda uusia kyberuhkia. Tätä toimintamallia kutsutaan panoptisismiksi (engl. panopticism), jossa kybertilannekeskuksen tavoitteena on saavuttaa täysi havaitsemiskyky paljastamatta omaa havaitsemiskykyään ulkopuolisille (Foucault 1995, 200-201). Havaitsemiskyvyssä on periaatteesta huolimatta aina katvealueita, joista tietoisena oleminen on tärkeää tilannekuvavinoutumien eli harhaluulojen välttämiseksi (Zimmerman 2014, 207). (Dasgupta ym. 2014, 68-69)

Toimintatapa (taso 4) kertoo, miten anturi tunnistaa kybermaailman tosiot eli tosiseikat jatkuvasta muutosvoimien eli bittien virrasta. Anturi voi esimerkiksi tunnistaa satelliitin ja puhelimen välisellä langattomalla siirtotiellä tai tietoliikennekaapelissa olevat jännite-erot niin sanotun johtokoodin avulla biteiksi. Näin fysikaalisesta signaalista saadaan radiovastaanottimen avulla muodostettu kyberavaruudessa ymmärrettäviä symbolisia ja tulkittavia eroavaisuuksia. (Dasgupta ym. 2014, 70; International Electrotechnical Commission 1993)

Toiminnallisuus (taso 5) määrittelee anturin toiminnan datan, symboleiden eli bittien käsittelemiseksi. Verkkoliikenteen anturit jaetaan toiminnallisesti **passiivisiin** ja **aktiivisiin** kyberavaruuden tilannetietojen kerääjiin. Verkkoliikenneanturien lisäksi kybertilannekeskuksen havaitsemiskyvyn laajentamiseksi voidaan käyttää sisällönsuodatukseen erikoistuneita palomuureja tai päätelaitteeseen asennettavia seurantaohjelmia. (Dasgupta ym. 2014, 70; Zimmerman 2014, 175-184 ja 207-212)

Passiivinen anturi välittää dataa eteenpäin tiettyyn määriteltyyn kyberavaruuden sijaintiin. Anturi saa datan esimerkiksi kaiken tietoliikenteen kopioivalta keskittimeltä (engl. network hub), lähiverkkoja siltaavalta kytkimeltä peilatusta portista (engl. switch port mirroring) tai verkkoliikenteen kuuntelulaitteelta (engl. network tap) (O'Kelly 2015, 235-236; Wang, Han & Jiang 2018). (Zimmerman 2014, 208)

Aktiivinen anturi sen sijaan voi muokata aktiivisesti dataa, muuttaa tarvittaessa sen muotoa, tehdä päättelyä ja estää määritellyn datan läpipääsyn. Aktiivinen anturi tarvitsee toimiakseen yhteyden erilliseen tai sisäänrakennettuun tunkeutumisen estojärjestelmään (IPS), joka ohjaa sen toimintaa. (Zimmerman 2014, 209) Lisäksi passiivisia kyberantureita voidaan

määritellä aistimaan tai ”kuulostelemaan” edunsaajan kyberavaruusalueen ulkopuolista liikennettä eli internetin ”taustakohinaa”. Haitallista liikennettä voidaan myös houkutella niin sanottuihin hunajaverkkoihin eli kyberansoihin. Tätä menetelmää käytetään hyökkääjien jatkuvasti muuttuvan toiminnan turvalliseksi tutkimiseksi, tutkimusdatan saamiseksi ja uusiin kyberuhkiin varautumiseksi (Fan, Du, Fernandez & Villagra 2017, 3906-3908).

Kyberanturi lähettää havaitsemansa datan eteenpäin määriteltyyn kohteeseen kyberavaruudessa *toimintaohjeiden* (taso 6) eli verkkoasetusten ja valitun protokollan eli siirtotavan avulla, jotta datan vastaanottajan on mahdollista tehdä datasta tulkintoja. Aisteilla saadun datan tulee olla tulkittavissa (taso 7), jolloin sillä on oltava tietty formaatti eli ”kieli” tai ”rakenne”, jotta käsittelijä voi ymmärtää sitä. (Dasgupta ym. 2014, 70-71) Tyypillisesti tilannetietoja keräävä tai vastaanottava kohde on järjestelmän oma lokituspalvelin, välityspalvelin, kybertilannekeskuksen turvallisuustapahtumien hallintapalvelu (engl. Security Incident and Event Management, SIEM) tai tunkeilijoiden tunnistus ja/tai estojärjestelmä (engl. Intrusion Detection/Prevention System, IDS/IPS). Data tallennetaan kaikissa tapauksissa lopulta tietokantaan tai lokitiedostoon eli ”muistiin”.

5.6 Esimerkkejä kyberavaruuden aistielimistä eli antureista

Palomuuri on yksi esimerkki kyberavaruuden aistielimestä eli teknisestä järjestelmästä, jolla voidaan estää asiattoman datan pääsy verkosta toiseen, kuten internetistä edunsaaja lähiverkkoon (Tietotekniikan termitalkoot 2007). Palomuurit jaetaan sovelluspalomuureihin ja laitepalomuureihin. Sovelluspalomuuri on päätelaitteeseen asennettava ohjelmisto, joka valvoo tietoliikenneyhteyksiä laitteen ja verkon välillä. Laitepalomuuri puolestaan valvoo tietoliikenneverkkojen välistä liikennettä. Palomuureista on olemassa kolmea eri sukupolvea: tilaton, tilallinen ja kolmannen sukupolven palomuuri. *Tilattoman palomuurin* toiminta perustuu ennalta määriteltyihin sääntöihin. *Tilallinen palomuuri* tarkastelee edellisen lisäksi aktiivisten verkkoyhteyksien toimintaa ja päättää historiatietojen pohjalta tietyn datapaketin läpipääsystä. Kiinnostavin kybertilannekeskuksen kannalta on *kolmannen sukupolven palomuuri*, joka yhdistää edellisiin ominaisuuksiin sovellustunnistuksen, sisällöntunnistuksen, pakettien avaamisen ”hiekkalaatikkotilassa”, tunkeutumisenestojärjestelmän (IPS) ja datan salauksen purun sisällön tarkastamiseksi. Jo tämäntyyppinen ratkaisu voi

tuottaa riittävästi dataa ja havaitsemiskykyä pienen kybertilannekeskuksen perustamiseksi. (Tuomaala 2018, 2-10; Winters 2019, 39)

Päätelaitteeseen asennettava seuranta- ja hallintaohjelma (engl. Unified Endpoint Management, UEM) mahdollistaa edunsaajan kyberavaruuteen kytkeytyvien laitteiden hallinnan esimerkiksi kybertilannekeskuksesta. Esimerkiksi puhelimiin, tietokoneisiin ja IoT-laitteisiin asennettavilla seuranta- ja hallintaohjelmilla voidaan tehdä turvallisuuspäivityksiä, muuttaa turvallisuusasetuksia, poistaa ja asentaa sovelluksia, poistaa varastetun tai hukkuneen laitteen tiedot, seurata laitteen toimintaa ja sijaintia, tarjota suojattuja virtuaalisia tunneloituja verkkoyhteyksiä (VPN) ja hallita kyberuhkia etäyhteydellä. Kybertilannekeskukselle päätelaitteiden seuranta ja hallinta mahdollistaa laajan havaitsemiskyvyn ja joustavan resilientin toiminnan eri tilanteissa. (Rouse 2018; TrustRadius 2019)

Erillisten seurantaohjelmien lisäksi monet sovellukset, palvelut ja laitteet rekisteröivät toiminnastaan itsenäisesti tilannetietoja ja tapahtumahistoriaa. Tällaisia palveluita ovat esimerkiksi käyttöjärjestelmät, sovellukset, tietokannat ja verkkokomponentit. Tilannetietojen keräämistapahtumaa kutsutaan lokitukseksi ja syntynyttä rekisteriä (tietokanta, tiedosto tai lokitusprotokolla) lokiksi. Lokitus voi sisältää tilannetietoja, kuten ajan, tapahtuman, toimijan, lähde- ja kohdeosoitteet ja käyttöoikeudet. Erityistä kyberturvallisuustapahtumiin erikoistunutta lokia kutsutaan auditointilokiksi (engl. audit log). (Margulies 2015, 84-85) Lokituksen laatu, määrä ja muoto vaihtelevat järjestelmäkohtaisesti, jolloin edunsaajaorganisaation eri palveluissa tuotettu lokidata tyypillisesti kerätään automaattisesti keskitettyyn lokienhallintasäilöön esimerkiksi SIEM-järjestelmiin (luku 5.8). Vaihtoehtoisesti lokitietoa voidaan tarkastella ja hakea käsin, joka on hyvin työlästä ja kasvattaa tilannevasteen aikaviivettä. (Madani, Rezayi & Gharaee 2011, 284-289)

5.7 Dataa, informaatiota ja tietämystä avoimista lähteistä

Edunsaajan kyberavaruuden todellisista tapahtumista voi saada luotettavan varmuuden ainoastaan kybermaailman havaitsemiskyvyn omaavien omien antureiden, palomuurien ja esimerkiksi päätelaitteisiin asennettavien seurantaohjelmien ja lokituksien eli primäärilähteiden avulla. Havaitsemiskyvyn laajuudesta riippuen on kuitenkin mahdollista, että primäärilähteistä havaitut tilannetiedot johtavat kybertilannekeskusta tilannekuvaa muodos-

tettaessa harhaan eli datan merkityksiä tulkitaan väärin tai data on ristiriitaista. Tästä johtuen kaikkien antureiden ei tarvitse olla kybertilannekeskuksen omia, vaan muiden tahojen luotettavia antureita ja ulkopuolisia lähteitä käytetään paljon. Tällaisesta kyberavaruuden muutosvoimista kertovan datan hankinnasta käytetään nimitystä ”avoimien lähteiden tiedustelu” (engl. Open-Source Intelligence, OSINT). (Joint Chiefs of Staff 2013, B-7 ja B-8)

Avoimien lähteiden tiedustelu on datan, informaation ja tiedon hankintaa tai vastaanottamista julkisista lähteistä, joiden dataresurssit ovat erikseen ostettavissa tai vapaasti saatavilla. Avoimen lähteiden tiedustelu kohdistuu toiskätiseen dataan eli sekundäärilähteisiin, jolloin lähteen luotettavuuden arviointi on tärkeää. Avoimista lähteistä saatavalla datalla voidaan varmentaa omien primäärilähteiden datan paikkansapitävyys tai avoimilla lähteillä voidaan saada dataa omien tilannetietoja tuottavien järjestelmien luotettavuudesta ja havainnoinnin kohdistamisesta oikealla tavalla. Sekundäärilähteet tuovatkin ”uuden näkökulman” käsillä olevaan tilanteeseen ja mahdollistavat tilannetietoisuuden oikeansuuntaisen kehittymisen varmistamisen. (Joint Chiefs of Staff 2013, B-7; Kivimäki 2017)

Luonnollisesti kaikki avoimista lähteistä saatava materiaali ei ole vain tässä tutkimuksessa määriteltyä dataa, vaan joukossa on myös jo datasta tulkittua informaatiota ja tietämystä. Avoimia lähteitä ovat fyysiset ja digitaaliset lähteet, jotka voidaan jakaa (1) massamediaan, (2) julkaisuihin, (3) rekistereihin ja (4) kuviin sekä videoihin. (Kivimäki 2017)

Massamediaa ovat esimerkiksi televisio, radio, lehdet ja internet-sivustot. Julkaisuja ovat esimerkiksi julkiset raportit, tutkimukset, kirjat, konferenssit, standardit ja kartat. Julkisia kyberavaruuden rekistereitä ovat esimerkiksi internetin IP-osoitteistopalvelimet (DNS) ja WHOIS verkkotunnustietokannat (Daigle 2004; Encyclopædia Britannica 2018a). Kuvia ja videoita edustavat kaikki vapaasti saatavilla olevat ja maksulliset kuvatietokannat, ilmakuvapalvelut, web-kamerat ja videopalvelut, kuten Kansalaisen karttapaikka ja Google Earth. (Joint Chiefs of Staff 2013, B-7; Kivimäki 2017)

Nämä lähteet voidaan saavuttaa esimerkiksi julkisissa kirjastoissa (kunnalliset ja yliopistot), internetin hakukoneilla (Google, Bing, Yahoo ja Baidu) sosiaalisella medialla (Facebook, WhatsApp, Instagram, Twitter, LinkedIn, IRC-kanavat, yms.) vertaisverkoilla (Freenet, GNUNet ja Skype) ja erilaisten julkisten kyberjärjestelmistä julkaistavan avoimen datan avulla (Bublitz & Hoffmann 2017, 3, 5, 213, 225; Encyclopædia Britannica 2018b; Jin & Chan 2010, 118; Manzanares-Lopez, Muñoz-Gea, Malgosa-Sanahuja & Sanchez-Aarnoutse 2010,

788-789 ja 794-795). (Kivimäki 2017) Esimerkiksi Googlen hakukoneella indeksoidun saatavilla olevan Internetin laajuus on satoja miljardeja verkkosivuja, jonka datan määrä on yli sata miljoonaa gigabittiä (Google 2019).

Internetissä on lisäksi paljon hakukoneiden ulottumattomissa olevaa indeksoimatonta, mutta saatavilla olevaa dataa niin sanotussa ”syvässä verkossa” (engl. deep web). Syvän verkon on arvioitu pitävän sisällään 90 prosenttia koko internetin koosta (Chandler & Munday 2016). Syvään verkkoon kuuluu esimerkiksi pieni pimeä verkko (engl. dark web), jonka tietoja on mahdollista tarkastella vain erillisillä sovelluksilla ja asetuksilla, kuten osapuolten anonymiteetin säilyttävällä Tor-verkon selaimella (Haraty & Zantout 2014, 415). Avoimen lähteiden dataa voidaan kybertilannekeskuksessa kerätä käsin eli manuaalisesti tai automaattisesti esimerkiksi tekoälyjärjestelmillä (engl. Artificial Intelligence, AI) ja hyödyntää saatua dataa tilannetietoisuuden muodostamisessa tiedon arvoketjussa. (Kivimäki 2017)

Lisäksi kybertilannekeskukset voivat kerätä tilannetietoja ja kehittää osaamista perinteisesti esimerkiksi puhelinsoitoilla, tekstiviesteillä, sähköpostilla ja kasvotusten keskustelemalla Näin voidaan toimia messuilla, yhteistyökumppanien tilaisuuksissa, viranomaisten järjestämissä kyberharjoituksissa ja tiedonvaihtoverkostoissa. Esimerkkinä Suomen valtion kyberturvallisuuskeskuksen koordinoimat toimialakohtaiset ISAC-tiedonvaihtoverkostot (engl. Information Sharing and Analysis Centre), jossa jaetaan tilannedataa, tilannekuvainformaatiota ja osaamista säännöllisissä luottamuksellisissa tapaamisissa. Tiedonvaihtoryhmiä on esimerkiksi ohjelmisto-, media-, pankki-, energia-, vesi-, sote-, valtionhallinto-, elintarvike-, internet-, kemia- ja metsäteollisuustoimialoille. (Kyberturvallisuuskeskus 2019) Kybertilannekeskustoiminnan kannalta verkostotoiminta on erittäin tärkeää, sillä ala kehittyy nopeasti ja kyberuhat sitäkin nopeammin.

5.8 Datan käsittelyn työkalut ja automatisointi

Datan määrä kyberavaruudessa kasvaa jatkuvasti. Edunsaajan kyberavaruuden havainnointiin on jo nykyään olemassa lähes täysin automatisoituja kybertilannekeskuksia, joissa ihmisen rooli on minimoitu virheiden välttämiseksi. Tällaisten keskusten ongelmana ovat erityisesti kalliit ylläpitokustannukset ja jäykkyys. Nykyaikaisessa kybertilannekeskuksessa yhdistyvätkin työkalujen automaation ja ihmistoiminnan osa-alueet. (Chamiekara ym. 2018,

100) Menestyvä kybertilannekeskus pyrkii jatkuvasti automatisoimaan rutiininomaisia tehtäviä, jotta vaikeampiin tapauksiin jää enemmän aikaa.

Kybertilannekeskuksen keskeisimpiä automaattisia tilannekuvajärjestelmiä ja työkaluja ovat esimerkiksi lokienhallinta ja turvallisuustapahtumien seurantaohjelmistot (SIEM), haavoittuvuus- ja verkkoskannerit, tunkeutumisen havainnointi- ja estojärjestelmät (IDS/IPS) ja verkkoliikennetallentimet.

Lokienhallinta- ja turvallisuustapahtumien seurantaohjelmistot (engl. Security Information and Event Management, SIEM) keräävät, kokoavat yhteen, suodattavat, priorisoivat ja etsivät riippuvuuksia datasta automaattisesti etukäteen määriteltyjen sääntöjen tai tekoälyn pohjalta. SIEMin tehtävänä on ottaa vastaan antureista saatu data ja muokata se määrämuotoiseen ja vertailtavaan formaattiin, tarjota reaaliaikainen pääsy tähän jäsenneltyyn dataan, suorittaa erillään olevien tapahtumien tehokasta synteesiä eli yhdistelyä ja tuottaa hälytyksiä toisistaan riippuvista tapahtumista. SIEM-järjestelmien etu perustuu datamassoista löydettävien tärkeiden riippuvuuksien löytämiseen ja tilannetietoisuuden kehittymisen tukemiseen. Nykyiset SIEM-järjestelmät vaativat kytkeytymistä antureiden datavirtaan, merkittävää työpanosta toisiinsa liittyvien hälytysten kontekstin tunnistamiseen ja reaaliaikaisten tilannetietojen seurantaa. Näiden haasteiden selättämiseksi on viime aikoina tehty tutkimusta itseohjautuvien ja mukautuvien SIEM-järjestelmien (engl. self adaptive SIEM) kehittelemiseksi. (Suarez-Tangil, Palomar, Ribagorda & Sanz 2015, 145-146)

Nämä uudet SIEM-järjestelmät yhdistävät dataa tehokkaammin tekoälytekniikoiden avulla. Esimerkiksi keinotekoisen neuroverkon avulla voidaan muuttuvasta kyberavaruuden datavirrasta luokitella pahantahtoisia toimintoja aiemmin kerätyn sisällön eli historiatiedon avulla yhdeksi hyökkäykseksi. Tämän jälkeen voidaan niin sanotun geneettisen ohjelmoinnin avulla muodostaa erilaisia kilpailevia tilannevasteita, joista parhaiten toiminut selviää ja heikoiten toimineet hylätään. Tämä periaate noudattaa biologiasta tuttua evoluution mekanismia parhaan ympäristöön liittyvän kelpoisuuden löytämiseksi ja mahdollistaa koneoppimisen. Edellä kuvattu uudentyyppinen SIEM-järjestelmä vähentää ihmisvoimin tehtävän työn määrää ja parantaa tilannetietoisuutta jopa automaattisen välittömän tilannevasteen tasolle asti parantaen kyberresilienssiä. (Suarez-Tangil ym. 2015, 145-155)

Haavoittuvuus- ja verkkoskannerit muodostavat joukon työkaluja, joiden toimintaperiaatteet vaihtelevat tapauskohtaisesti. Yleisesti haavoittuvuusskannerit (esimerkiksi ”Nessus”)

luotaavat edunsaajan kyberavaruutta aktiivisesti (engl. active probing) ja testaavat, kuinka erilaiset laitteet, palvelut ja komponentit reagoivat erilaisiin kyselyihin eli ärsykkeisiin (Dusia & Sethi 2018, 1-3). Tämän perusteella saadaan dataa vioista ja vääristä asetuksista verkon viiveiden, häviöiden ja datan reittien avulla (Natu & Sethi 2006, 25). Haavoittuvuusskannerit voivat etsiä myös vanhentuneita ja päivittämättömiä sovellusohjelmia ja oletussalasanoja. Tehokas edunsaajaorganisaation haavoittuvuusskannaus on jatkuvaa toimintaa kertaluonteisen toimintatavan sijaan (Berlin & Brotherston 2017, Vulnerability Management). Verkkoskannerit (esimerkiksi ”NMap”) puolestaan luotaavat edunsaajan kyberavaruudesta löytyviä palveluportteja ja kartoittavat verkon eri osat tilannekuvan luomista varten. Verkkoskannerit voivat esimerkiksi tunnistaa laitteiden käyttöjärjestelmäversiot ja varoittaa uusista verkkoon kytketyistä tunnistamattomista laitteista. (Jetty 2018, Various features of NMap)

Tunkeutumisen havainnointi- ja estojärjestelmät (engl. Intrusion Detection/Prevention System, IDS/IPS) ovat kyberavaruuden tarkkailuun käytettyjä työkaluja, jotka seuraavat kybertilannetietoja laitteisiin asennettuina sovelluksina tai verkkoliikenteeseen kytkettyinä laitteina. IDS ja IPS järjestelmien toiminta perustuu (1) datapakettien allekirjoituksiin eli pahantahtoisen verkkoliikenteen tuntomerkkien eli ”sormenjälkien” etsintään tai (2) anomalioihin eli poikkeavuuksiin edunsaajan kyberavaruuden normaalitilanteesta. (Zimmerman 2014, 121-122) IDS ja IPS järjestelmät eroavat toisistaan siten, että IDS toimii passiivisesti havainnoimalla verkkoliikennettä, kun IPS voi lisäksi estää verkkoliikenteen kulkua ja siten tehdä automaattisen tilannevasteen etukäteen tehdyn päätöksen eli sääntöjen perusteella. IPS voidaan myös sulauttaa palomuuriin, kuten edellä kuvatussa kolmannen sukupolven palomuuriratkaisussa. (Berlin & Brotherston 2017, IDS and IPS)

Huolimatta edellisistä toimintaa automatisoivista järjestelmistä, on monesti hyödyllistä tallentaa kaikki verkkoliikenne tietyltä aikaväliltä niin sanottujen verkkoliikennetallentimien avulla (PCAP). Nämä ohjelmistot tai laitteet toimivat siten, että niihin tallentuu tietyltä määritetyltä aikaväliltä kaikki verkkoliikenne, jota voidaan myöhemmin tarkastella. Tarve tarkastella voi johtua esimerkiksi isosta kyberuhan toteutumisen tutkinnasta, oikeudellisista syistä ja jo toteutuneen tilanteen tarkan analysoinnin tarpeesta. Analysoinnissa käytetään esimerkiksi ”WireShark” pakettienanalysointiohjelmaa. (Zimmerman 2014, 130-132)

5.9 Työntekijöiden toiminnan luokittelu

Datan kerääminen erilaisiin työkaluihin on kybertilannetietoisuuden näkökulmasta turhaa, jos sitä ei jalosteta tiedon arvoketjussa korkeammalle asteelle. Kybertilannekeskus on paikka, jossa aistitasojen kautta datasta koostuvat tilannetiedot havaitaan ja niille annetaan merkityksiä. Tässä prosessissa jalostuu informaatiota – tilannetiedoista muodostetaan tilannekuvaa. Tilannekuvan muodostumista voidaan tukea automaatiolla, mutta viime kädessä tilannekuva muodostuu ihmisen tulkinnan kautta subjektiivisesti. Tämä johtuu automaattisten järjestelmien heikkoudesta ennustaa tulevia tapahtumia, jolloin syntyy paljon vääriä ja vähän oikeita hälytyksiä. Osa hälytyksistä jää automaattisesti huomaamatta. (Demertzis, Kikiras, Tziritas, Sanchez & Iliadis 2018, 1 ja 11-12; Zimmerman 2014, 36-38) Tällöin tärkeäksi elementiksi nousevat automaation lisäksi erilaiset organisatoriset prosessit, joilla dataa ja tilannekuvainformaatiota tarkastellaan kriittisesti ja jatkojalostetaan tiedon arvoketjussa kohti tilannetietoisuutta sekä oikeaa tilannevastetta.

Kybertilannekeskuksen tilanteenmukaisen resilientin, aikakriittisen ja paineisessa tilanteessa toimimisen perustan luovat ihmiset eli kybertilannekeskuksen työntekijät ryhmänä osana organisaatiota (Hámornik & Krasznay 2018, 244). Kybertilannekeskuksessa työskentelee kyberturvallisuusalan asiantuntijoita erilaisin kokemuksin ja painotuksin. Asiantuntemusalueita ovat esimerkiksi tietoliikenne, tietoverkot, palomuurit, data-analyysi, käyttöjärjestelmät, alustat, turvallisuustestaus, asiakaspalvelu, strateginen johtaminen, konsultointi ja uhkatiedustelu. Tehtävänimikkeitä ovat muun muassa tilannepäivystäjä, asiakastuki, tilannekoordinaattori, tekninen ylläpitäjä, taktikko, vuoropäällikkö, johtaja, sihteeri, tiedustelija, forensikko ja ohjelmistokehittäjä. Yksi työntekijä voi toimia monissa rooleissa. Tehtävät jakautuvat kybertilannekeskuksen tehtävien laajuudesta riippuen yksiköihin eli osastoihin, jotka yhdessä muodostavat kybertilannekeskuksen organisaation. (Demertzis ym. 2018, 1-3)

Osastot voidaan jakaa (1) operatiivisiin, (2) taktisiin ja (3) strategisiin toiminnan laadun ja päätöksenteon mukaisesti. Operatiivinen toiminta on lyhyen aikavälin päivittäistä tai viikoittaista edunsaajan kyberavaruuden tilanteenmukaista päätöksentekoa, aikatauluttamista ja resurssien käyttämistä. Taktinen toiminta on keskipitkän aikavälin suunnittelua, resurssitarpeiden mitoittamista ja varautumista erilaisiin edunsaajan kyberavaruuden toi-

minnan jatkuvuutta uhkaaviin häiriöihin. Strateginen toiminta on pitkän aikavälin kybertilannekeskuksen tavoitteiden, toiminnan laajuuden, rakenteiden ja edunsaajan tarpeiden kartoittamista. Lisäksi strategiseen toimintaan kuuluu resursseista päättäminen. (Muñoz ym. 2012, 397-399; Sahebjamnia ym. 2015, 264)

Osastoja voidaan luokitella lisäksi hallintakeinojen ajallisen painotuksen mukaisesti ehkäisevään (engl. deterrent), ennakoivaan (engl. proactive), reagoivaan (engl. reactive) ja takautuvaan (engl. retrospective). Ehkäisevät ja ennakoivat hallintakeinot ovat kyberuhkaan nähden etukäteisiä. Reagoivat ja takautuvat puolestaan jälkikäteisiä. Ehkäisevät hallintakeinot pyrkivät estämään kyberuhkien toteutumisen. Ennakoivat hallintakeinot ovat kyvykkyyksiä, joilla varaudutaan joustamaan ja mukauttamaan toimintaa kyberuhan toteutuessa. Reagoivat hallintakeinot ovat reaaliaikaisia ja joustavia toimia jo toteutuneen kyberuhan vaikutusten vähentämiseksi ja jatkuvuuden varmistamiseksi. Jälkikäteiset hallintakeinot ovat toimia kyberuhan vaikutuksista palautumiseksi. (Onwubiko 2015, 8-10; Zimmerman 2014, 14) Parhaassa tilanteessa kybertilannekeskuksessa käytetään kaikkia edellä esitettyjen hallintakeinojen ajallisia painotuksia etukäteisyyttä korostaen.

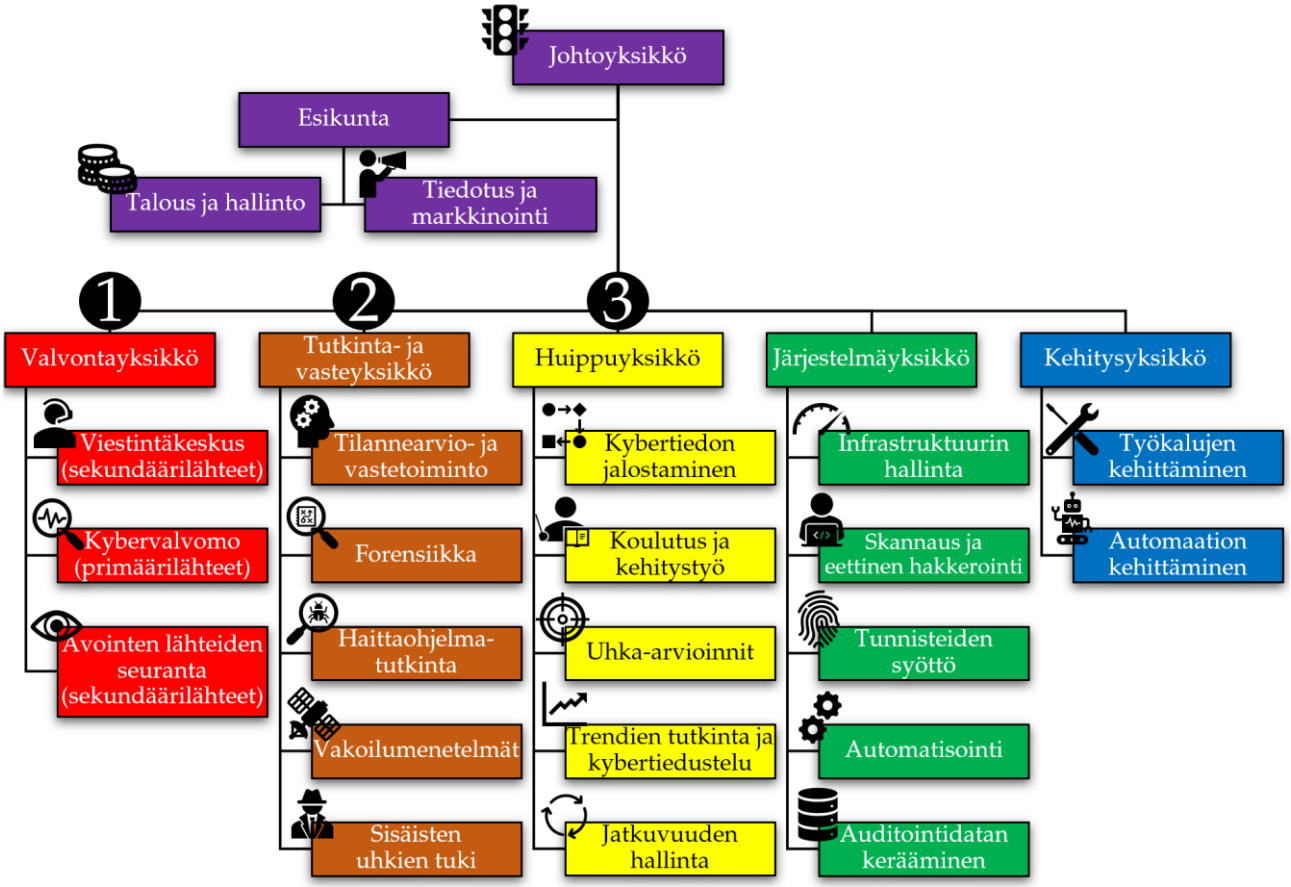
5.10 Tilannetietoisuuden muotoutuminen, tasot ja yksiköt

Kybertilannekeskuksen osastojen roolia voidaan tarkastella tasoittain (engl. tier), jotka jaotellaan datan käsittelyn ensisijaisuusmäärittelyn (engl. triage) perusteella (Brown, Greenspan & Biddle 2016, 697; Zimmerman 2014, 11). Triage-menetelmää käytetään esimerkiksi suurten onnettomuuksien ja kriisien yhteydessä potilaiden priorisoimiseksi silloin, kun resurssit ovat rajalliset (Christian ym. 2014, e63S). Huolimatta kyberturvallisuuden erityispiirteistä, kuvattava prosessi noudattelee pääpiirteissään minkä tahansa hätätilanteen hoitamisen kaavaa. Alla eräs esimerkki.

Asiakas soittaa hätänumeroon 112 ja välittää dataa, jonka perusteella päivystäjä (taso 1) tekee arvion jatkotoimenpiteistä ja hälyttää tarvittaessa erillisen yksikön suorittamaan tehtävää. Tämä erillinen yksikkö (taso 2) voi olla esimerkiksi palokunnan sammutusyksikkö, joka sammuttaa tulipalon. Tämän jälkeen palonsyyntutkintaa varten hälytetään poliisi paikalle (taso 3) suorittamaan rikosoikeudellinen tutkinta tapahtuneesta.

Edellisten tasojen lisäksi keskukseen tarvitaan järjestelmiä ylläpitäviä ja kehittäviä yksiköitä ja hallinnollinen johtoyksikkö. Monissa kybertilannekeskuksissa on vain osa seuraavassa

esitettävistä ison keskuksen toiminnoista ja toimintoja on järjestetty eri keskuksissa eri tavoin (kuvio 22). (Norri-Sederholm 2015, 43-44; Zimmerman 2014, 10)



Kuvio 22. Kybertilannekeskusorganisaation mallihierarkia ja toiminnan osastojako (Zimmerman 2014, 54 ja 57). Osastojako on käytännössä hyvin vaihteleva eri kybertilannekeskuksissa toiminnan laajuuden ja palvelusuuntautumisen mukaisesti.

Kybertilannekeskuksen ensimmäistä tasoa kuvaa operatiivinen **valvontayksikkö** (kuviossa 22 punaisella, **taso 1**). Valvontayksikkö pitää sisällään reaaliajassa ihmisiltä tulevaa dataa varten viestintäkeskuksen (engl. help desk, support tai front line), edunsaajan kyberavaruuden havainnointia varten kybervalvomon ja avointen lähteiden seurannan toiminnot (Brown ym. 2016, 697). Näissä toiminnoissa työskentelevä kybertilannekeskuspäivystäjä, -operaattori tai asiantuntija havainnoi kyberavaruuden muutosvoimia erilaisten työkalujen, näyttöruutujen ja viestivälineiden välityksellä ja tekee operatiivisia päätöksiä muutosvoimien hallitsemiseksi (Onwubiko 2018, 5). Operatiivista kokonaisuutta valvoo tilannekuvakoordinaattori, vuoropäällikkö tai ylipäivystäjä, joka toimii lähiesimiehenä tai työnjohtajana ja valvoo resurssien järkevää käyttöä.

Ensimmäisen tason (**taso 1**) tehtävänä on luokitella tapahtumia. Yksinkertaisissa ja vähän aikaa vievissä tapauksissa ne ratkaistaan jo tällä tasolla. Merkityksellisiksi katsotut tapahtumat kirjataan asiankäsittelyjärjestelmään (ns. tiketti- tai keikkajärjestelmä), jossa niille annetaan ensisijaisuusarvo tai vakavuusaste. Tämä arvo kuvaa käsittelijän (päivystäjä, operaattori, asiakaspalvelija) tulkintaa datan merkittävyydestä erikseen annettujen kriteerien, arvosteluasteikon tai riskinarvion perusteella. Alhaisimmat vakavuusarvot (esim. 1-2) liittyvät tyypillisesti esimerkiksi yksittäisiin työasemiin ja vakavammat (esim. 3-5) laajempiin verkkohäiriöihin tai palveluiden alasajoon. Päätöksen tekeminen voi perustua induktiiviseen tai deduktiiviseen päättelyyn, hahmontunnistukseen, hypoteeseihin ja intuitioon (Manchester Triage Group 2015, 8-9). Käsittelijä voi yhdistää käsillä olevan tapahtuman aiemmin havaittuun tapahtumaan ja määritellä mihin edunsaajan kyberavaruuden osaan tapahtumalla voi olla vaikutuksia ja mihin tapahtuma kohdistuu. Asian jatkokäsittelyn nopeuttamiseksi voidaan lisäksi päättää, mikä taho jatkaa tarvittaessa asian selvittämistä. Samalla alkuperäisen datan ympärille muodostuu informaatiota ja tilannekuva täydentyy. Käsittelijä voi kirjata ylös kokemuksiin, tietotaitoon ja kyvykkyyteensä perustuen tilanteen ymmärtämisessä auttavia asioita. Datan tullessa ihmiseltä (esimerkiksi viestintäkeskukseen puhelimitse), voidaan antaa välittömiä toimintaohjeita asian ratkaisemiseksi. (Norri-Sederholm 2015, 43-44) Tyypillisesti tason 1 käsittely voi kestää enintään 15 minuuttia edunsaajan kyberavaruuden ja resurssien laajuuden mukaisesti. Tätä kauemmin aikaa vievät tilanteet välitetään yksiköille tasolla 2. (Onwubiko 2018, 5; Van der Kleij, Kleinhuis & Young 2017, 5; Zimmerman 2014, 11)

Operatiivinen **tutkinta- ja vasteyksikkö** (kuviossa 22 oranssilla, **taso 2**) on erityisasiantuntijoista koostuva osasto, jonka tehtävänä on ratkaista edunsaajan kyberavaruuden ongelmia muodostamalla tilanneymmärrystä ja tekemällä viisaita päätöksiä tilannevasteen toteuttamiseksi ja asian ratkaisemiseksi oikealla, nopealla ja tehokkaalla tavalla. Jokainen valvontayksiköltä saatu tapaus käsitellään tietyssä tavoitteellisessa vasteajassa ja tietyllä laajuudella palvelutasosopimuksen (engl. Service Level Agreement, SLA) mukaisesti (Zimmerman 2014, 11). Tutkinta- ja vasteyksikkö ei toteuta reaaliaikaista havainnointia, vaan keskittyy tapausten selvittämiseen. (Zimmerman 2014, 11)

Tutkinta- ja vasteyksikkö koostuu tilannearviotoiminnosta, jossa kyberturvallisuusalan tekniset asiantuntijat määrittelevät valvontayksiköltä saadun ja itse hankitun tilannekuvain-

formaation pohjalta yhteisen ymmärryksen tapahtuneesta. Ymmärryksen luomisessa käytetään tyypillisesti synteesin ja analyysin menetelmiä. Synteesissä erillistä informaatiota yhdistellään asiakokonaisuuksittain ja synteesi sisältää usein johtopäätöksiä. Analyysi puolestaan on hyödyllistä, mikäli isosta jo tunnetusta tapahtumasta halutaan kokonaisuutta erittelemällä, purkamalla ja taustaoletuksiin palauttamalla saavuttaa tarkempi ymmärrys. (Tieteen termipankki 2019d) Ymmärrys pohjautuu asiantuntijoiden omaan taitoon, kokemukseen, koulutukseen ja kykyihin.

Kybertilannekeskuksella voi olla omat erityisosastonsa esimerkiksi forensiikasta (rikosten ja tapahtumien jäljitys), haittaohjelmien tutkinnasta, vakoilumenetelmien tuntemuksesta ja edunsaajan sisäisten kyberuhkien selvittämisestä (Santos, Muniz & De Crescenzo 2017, 2.forensics). Tästä syystä tutkinta- ja vasteyksikössä on tyypillisesti kokenutta, koulutettua ja osaavaa henkilökuntaa. (Zimmerman 2014, 57) Henkilökunnan taitotaso on resilienssin yksi tärkeä tekijä.

Tilannearviotoiminnon yhteydessä toteutetaan tilannevaste (**taso 2**) eli päätös siitä, millä kyberavaruuden muutosvoimien hallitsemiseksi käytettävissä olevilla kyvykkyyksillä eli hallintakeinoilla haitallinen tilanne korjataan. Tilannevasteella pyritään mukautumaan kyberavaruuden muutoksiin siten, että edunsaajan kybertoiminnan jatkuvuus voidaan turvata ja palautuminen tapahtumasta aloittaa mahdollisimman nopeasti. Tyypillisesti tilannevasteen tuottamiseen menee vaikeimmissa tapauksissa aikaa tunneista jopa viikkoon. (Zimmerman 2014, 11)

Huippuyksikkö on strateginen ja taktinen (kuviossa 22 keltaisella, **taso 3**) tutkimusyksikkö, joka tuottaa tilanneymmärrystä jalostamalla valvonta- ja tutkintayksikön tuottamaa tietämystä hyödylliseen muotoon tiedustelutuotteiksi (raporteiksi, kuvaajiksi, kaavioiksi), jotka hyödyttävät kybertilannekeskusta toiminnan kehittämisessä ja edunsaajaorganisaation ylintä johtoa päätöksenteossa. Huippuyksikkö tuottaa tasolta 2 saadun tilanneymmärryksen pohjalta pitkän aikavälin tilannetietoisuuteen liittyviä ratkaisuja, tutkii kybertilannekeskuksen sisäisiä prosesseja ja pyrkii ehkäisemään kehittyneiden pitkäkestoisten kyberuhkien (engl. Advanced Persistent Threat, APT) toteutumista. Huippuyksikkö voi esimerkiksi kouluttaa ja perehdyttää työtekijöitä. Huippuyksikön tehtävänä on ennustaa edunsaajan ja sen ulkopuoliseen kyberavaruuteen kohdistuvia muutosvoimia – trendejä – ja luoda uhka-arvi-

oita varautumisen tueksi. Huippuyksikkö voi lisäksi tarjota konsultointi- ja asiantuntijapalveluita esimerkiksi edunsaajan jatkuvuussuunnittelun (engl. Business Continuity Plan, BCP) ja toipumissuunnittelun (engl. Disaster Recorvery Plan, DRP) tueksi. (Zimmerman 2014, 56-57)

Järjestelmäyksikkö (kuvio 22) on operatiivinen valvontayksikön tukiyksikkö, joka mahdollistaa operatiivisen tilannetietoisuustoiminnan. Järjestelmäyksikössä ei luoda valvontayksikön tavoin tilannetietoisuutta, vaan pikemminkin säädetään ja parannellaan edunsaajan kyberavaruuden aistitasoja eli pidetään huolta kybertilannekeskuksen ”näkökyvystä” kyberavaruuteen. Järjestelmäyksikön tehtävänä on luoda ja ylläpitää mahdollisimman korkeaa kyberavaruuden havaitsemiskykyä, suojata kybertilannekeskuksen oma toiminta sekä tunnistaa ja korjata vikoja kybertilannekeskuksen omissa järjestelmissä. Työntekijät ovat tyypillisesti teknisiä ylläpitohenkilöitä, joilla voi olla esimerkiksi verkkoyhteys, SIEM, IDS/IPS ja erilaisiin haavoittuvuusskannereihin liittyvää osaamista.

Järjestelmäyksikön toimintoja ovat muun muassa infrastruktuurin, kuten palvelimien, verkkoyhteyksien ja ohjelmistojen hallinta ja ylläpito. Lisäksi osaamisesta riippuen jatkuvana vikojentunnistamistoimintona voi olla kybertilannekeskuksen omien verkkojen skannaus tai edunsaajan verkon skannaus palveluna. Lisäksi voidaan suorittaa niin sanottua ”eettistä hakkerointia”, jossa hakkereiden käyttämillä menetelmillä testataan kybertilannekeskuksen hyökkäyksenkestävyys ja samalla simuloidaan edunsaajan verkkoon mahdollisesti tulevia hyökkäyksiä ja korjataan haavoittuvuuksia etukäteen (Taskinen 2018, 47-48). Tunnisteiden syöttämistoiminto liittyy haitallisten muutosvoimien tunnistamiseen esimerkiksi haitallisen dataliikenteen sormenjäljistä, allekirjoituksista tai tunnisteista. Jatkuvan automatisoinnin lisääminen on edellytys toiminnan kehittämiselle, jotta valvontayksikön rutiininomaisten ja samalla tavalla toistuvien tehtävien hoitamista voidaan nopeuttaa ja aikaviivettä tilannevasteen tuottamiseksi pienentää. Järjestelmäyksikön tehtävänä on myös kerätä tietoa kybertilannekeskuksen toiminnasta mahdollisten väärinkäytöstapausten ja sisäisen tutkinnan varalle. (Zimmerman 2014, 54)

Kehitysyksikkö (kuvio 22) on taktinen valvonta sekä tutkinta- ja vasteyksikön tukiyksikkö, jonka tehtävä on kehittää räätälöityjä työkaluja ja automaatiota kybertilannekeskustoiminnan helpottamiseksi. Kehitysyksikössä työskentelevät tyypillisesti ohjelmistokehittäjä, koodarit, ohjelmistotestaajat ja projektipäälliköt. (Zimmerman 2014, 56-57)

Johtoyksikkö ja **esikunta** (kuvio 22) on strateginen ja taktinen yksikkö, jonka tehtävänä on ohjata kybertilannekeskuksen pitkän aikavälin toimintaa ja huolehtia edunsaajan tarpeiden täyttymisestä kyberresilienssin osalta. Esikunnassa tuotetaan hallintotoimintaan liittyviä tukitehtäviä ja tiedotetaan tarpeellisin osin toiminnasta julkisuuteen. Johtoyksikkö voi tarvittaessa tarjota konsultointia esimerkiksi kriisijohtamistilanteissa isojen häiriöiden toteutuessa. Johtoyksikössä työskentelevät kyberturvallisuuden asiantuntijat, joilla on johtamiskokemusta tai koulutusta ja kykyä johtaa ihmisiä kriisitilanteessa. Lisäksi yksikössä toimivat johtoryhmä, tiedottaja ja muut tarvittavat hallinnollisissa tehtävissä toimivat henkilöt. Tarvittaessa johtoyksikkö voi määrätä erillisen työ- tai kriisiryhmän isojen kriisitilanteiden selvittämiseksi. Ryhmälle voidaan nimittää erityinen tilannejohtaja koordinoimaan selvittämistä, tiedottamista, palautumista ja tietojen keruuta.

Huolimatta edellä määritellystä osastojaosta, on tyypillistä, että varsinkin tasoilla 1 ja 2 toimivat työntekijät toimivat vuorotellen kiertävästi erilaisissa tehtävissä. Näin voidaan kehittää ja monipuolistaa työtehtäviä sekä lisätä arvokasta kokemusta työntekijöiden keskuudessa. Osaamisen kasvattaminen on tärkeää etenkin työntekijöiden pitämiseksi organisaation käytössä, sillä kilpailu osaajista on alalla kovaa (Van der Kleij ym. 2017, 5).

Edellä kuvattu valvontayksikkö (**taso 1**) muodostaa kybertilannekeskuksen rungon, joka voi tarvittaessa toteuttaa ympärivuorokautisen (24/7), virka-aikaisen (8/5) tai tiettyinä aikoina palvelevan päivystyspalvelun. Palvelun laajuuden määrittely on edunsaajan tarpeista kiinni. Lainsäädäntö (esimerkiksi GDPR ja NIS -direktiivit), toiminnan ja kohteen luonne (jatkuva vai aukioloaikoihin perustuva), resurssit (raha, osaava työvoima) ja jatkuvuuskysymykset määrittelevät palvelutason (SLA) määrittelyn. Tutkinta- ja vasteyksikkö (**taso 2**) voi toimia vajaalla päivystyksellä iltaisin ja öisin tai ainoastaan päiväaikaan. Taso 1 on yleensä aina riippuvainen ylempien tasojen ja tukiorganisaatioiden tuesta. Tyypillisesti huippu-, järjestelmä-, kehitysyksiköt toimivat ainoastaan päiväaikaan. Suurimmilla organisaatioilla voi olla monia kybertilannekeskuksia ympäri maailmaa, jotka vastaavat kukin omalla päivävuorollaan ja siirtävät vastuun seuraavalle kybertilannekeskukselle tiettynä kellonaikana. (Onwubiko 2015, 5)

Kybertilannekeskuksen päivittäisen toiminnan tasoa voidaan kuvata maturiteetin käsitteellä, joka tarkoittaa tilannetietoisuustoiminnan kypsyystasoa eli kykyisyyttä. Maturiteet-

tiin vaikuttavat esimerkiksi laitteiston taso, järjestelmien kytkeytyneisyyden aste, henkilöstön osaaminen ja kokemus, henkilöstövaihtuvuuden sujuvuus, henkilöstön sitoutuminen ja työyhteisön toimivuus.

5.11 Tilannehuone eli ”war room”

Valvontayksikkö toimii tyypillisesti fyysisesti yhteisessä suojatussa teknisillä kyberavaruuden havainnoinnin mahdollistavilla laitteilla varustetussa rauhallisessa tilassa, jota kutsutaan tilannehuoneeksi, tilannekeskukseksi tai komentokeskukseksi eli ”war roomiksi”. Tilaan ei tyypillisesti pysty näkemään ulkopuolelta ja se on erillisessä kulunvalvotussa huoneessa. Vain tilannehuoneen taustatarkistetulla henkilöstöllä on pääsy tilannehuoneeseen. Tilannehuoneelle tulee olla määritelty varatila, mikäli tilan käyttö on estynyt. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 52-53)

Kuva 1. Traficomin Kyberturvallisuuskeskuksen tilannekeskuksen esittelymateriaalissa valvontayksikön työntekijät luovat tilannekuvaa ja jakavat sitä isoilla näyttöruuduilla. (Traficom 2018, 15)

Tilan tekninen varustelu muodostuu edunsaajan tietoliikenneyhteyksien lisäksi erillisestä varmennetusta internetyhteydestä ja sähkövirtavarmennuksesta sähkökatkosten ajaksi. Tilan isoimmalle seinälle voi olla asennettu valkotaulujen, videotykkien ja näyttöjen avulla jaetun tilannekuvan muodostamisessa auttavia virtuaaliseiniä (kuva 1). Rakennusteknisesti tilalle voi olla määritelty erilaisia suojatoimia esimerkiksi äänieristys ja rakenteet hajasäteilyä (TEMPEST) ja murtautumisia vastaan. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 52-53)

Huoneessa voi olla päätetyöpisteitä sijoitettuna auditoriomuodostelmaan eri korkeuksille siten, että jokaiselta pöydältä voi nähdä jaetun tilannekuvan näyttötaulut helposti. Työpisteillä on mahdollisuus useampien näyttöruutujen käyttämiseen ja oman kannettavan tietokoneen kytkemiseen helposti tilannekuvan jakamiseksi muille työntekijöille (kuva 1) Keskuksen ollessa isompi, voi käytössä olla myös kuulokemikrofonien avulla toimiva puhekommunikaatiojärjestelmä. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä 2016, 52-53)

Kybertilannekeskuksia on ollut erilaisissa muodoissaan Suomessa olemassa jo ainakin 2000-luvun alusta lähtien. Tilannehuoneita on sijoiteltu Suomessa yksityisten yritysten ja julkisten viranomaisten tiloihin ja niiden määrä on 2010-luvulla kasvanut jatkuvasti. Tilan vaatimukset ja toteutukset vaihtelevat toiminnan laadun mukaan laajasti pienistä ja vaatimattomasti varustelluita konttoreista suuriin ja räätälöityihin tilannehuoneisiin. 2020-luvulle mentäessä useita kybertilannekeskuksia laajennetaan ja toimintaan rekrytoidaan asiantuntijoita. Kybertilannehuoneiden fyysisen sijainnin merkitys on pienentynyt tietoliikenneyhteyksien parantuessa ja tärkeimmäksi sijoitustekijäksi on tullut henkilöstön saatavuus.

6 AINEISTOANALYYSI

Tässä luvussa analysoidaan tutkimusprosessin aikana kerätty haastatteluaineisto sitaattianalyysin ja teemoittelun keinoin. Tekstin joukkoon on nostettu asiantuntijoiden esittämiä litteroituja kommentteja, jotka todistavat luvussa kuvattavien tulosten olemassaolon. Aluksi kuvataan aineistonkeruumenetelmän toteuttaminen, haastateltavien profiilit ja haastatteluolosuhteet.

6.1 Asiantuntijahaastattelut

Tutkimusraportin menetelmävalintaosuudessa kuvattuun tutkimuskysymykseen vastaamiseksi ja teoriataustan sopivuuden varmistamiseksi on tämän tutkimuksen yhteydessä kerätty tutkimusaineisto asiantuntijahaastatteluilla. Puolistrukturoidun teemahaastattelun kysymysrunko on kuvattu tutkimusraportin liitteessä 1. Teemahaastattelussa oli viisi teemaa: kyberturvallisuus, käsitteet, kybertilannekuva, kyberresilienssi ja kybertilannekeskus. Teemojen lisäksi haastattelurunkoon koostettiin tutkimusongelmaan liittyviä tarkentavia kysymyksiä ja esimerkkejä aikaisemmista tutkimuksista. Haastattelurungon kysymysten reliabiliteetti ja validiteetti tarkastutettiin tutkimuksesta riippumattoman kyberturvallisuuden asiantuntijan toimesta, jonka pohjalta tehtiin korjauksia kysymyksiin. Palautteen pohjalta haastattelulomakkeeseen lisättiin muutamia tarkentavia kysymyksiä, kysymysten muotoiluja muutettiin ja järjestystä vaihdettiin.

Varsinainen **haastattelu** suoritettiin Cyber Security Nordic -messuilla Helsingin messukeskuksessa kahtena päivänä 10. -11. lokakuuta vuonna 2018. Haastateltavat valittiin etukäteen tehdyn *organisaatioanalyysin* ja paikan päällä tehtyjen *taustakartoitusten* perusteella.

Organisaatioanalyysissä tunnistettiin messuilla olevien organisaatioiden kypsyyttä kybertilannekeskustoimintaan organisaatioiden internet-sivujen ja muiden julkisten lähteiden pohjalta. Jokainen messuille osallistunut organisaatio arvioitiin ja järjestettiin listaan arvioidun kybertilannekeskusosaamisen perusteella. Organisaatioiksi valittiin julkisia ja yksityisiä organisaatioita.

Paikan päällä suoritettu **taustakartoitus** toteutettiin tiedustelemalla kybertilannekeskustoiminnasta vastaavaa tai toiminnan tuntevaa henkilöä haastateltavaksi valittujen organisaatioiden messupisteellä. Haastateltuja asiantuntijoita oli yhteensä seitsemän. Kaikilla haastatelluilla oli pitkä kokemus kyberturvallisuusalalta. Haastateltujen päivittäiset työtehtävät liittyivät kybertilannekeskustoimintaan ja aihealueen tuntemus varmistettiin alustavilla kysymyksillä. Näistä alustavista kysymyksistä on koostettu pseudonymisoidut eli tunnistetiedoista riisutut profiilit taulukoon 2. Haastateltavista kolmella oli 5-10 vuoden, kahdella 10-15 vuoden ja kahdella 15-20 vuoden työkokemus kybertilannekeskustoiminnasta. Kokeneimmat haastateltavat olivat työskennelleet kybertilannekeskusta vastaavassa organisaatiossa jo vuodesta 1999.

№	Toimenkuva	Organisaatiotyyppi	Kokemus vuosina	Kokemuksen kuvaus
1	Toimitusjohtaja	Yksityinen	8	Kansallinen kyberturvallisuustyö.
2	Tietoturva-asiantuntija	Yksityinen	6	Maaliosasto- ja hyökkäyssimulaatiotoiminta.
3	Tietoturvakonsultti	Yksityinen	6	Kybertilannekeskuksiin liittyvät kartoitukset.
4	Tietoturvavastaava ja -päivystäjä	Yksityinen	19	Kybertilannekeskuksen suunnittelu ja perustaminen kaksi kertaa.
5	Tilannekeskusasiantuntija	Yksityinen	19	Tilannevastetoiminta ja harjoitukset.
6	Tilannepäivystäjä	Julkinen	13	Operatiivinen päivystys.
7	Tilannekoordinaattori	Julkinen	12	Yhteistyöverkostot ja isojen kyberhäiriöiden johtaminen.

Taulukko 2. Haastateltujen asiantuntijoiden profiilit pseudonymisoituna.

Haastateltaviksi valittiin sekä organisaatioiden ylintä johtoa, että käytännön työtä tekeviä asiantuntijoita. Lisäksi haastateltaviksi valittiin sekä yksityisen, että julkisen sektorin tieto- ja kyberturvallisuusalan organisaatioissa työskenteleviä, jotta haastatteluaineisto olisi mahdollisimman kattava ja läpileikkaisi kybertilannekeskusten toimintaa molemmista näkökulmista. Haastateltujen työtehtäviä olivat muun muassa toimitusjohtaja, tietoturva-asiantuntija, tietoturvakonsultti, rahoituslaitoksen tietoturvavastaava, finanssialan varautumissuunnittelija, tilannekuvakoordinaattori ja tilannepäivystäjä. Haastateltujen erityisosaamisalueita olivat muun muassa kyberturvallisuusstrategiatyö, hyökkäyssimulaatiot (ns. ”red team” -toiminta), CSOC-kartoitukset, kyberturvallisuuskoordinointi, kybertilannekeskustoiminta, isojen kybertilanteiden tilannekuvakoordinointi ja yhteistyö kybertilannekuvan luomisessa. Kybertilannekeskustoiminta oli haastatelluille tuttua työtehtävien ja harjoitusten kautta. Osa haastatelluista oli tehnyt operatiivista kybertilannekeskuspäivystystä ja osa

koordinoinut kybertilannekeskuksen perustamista tai jatkuvaa toimintaa ja sen kehittämistä.

Haastattelutilanne nauhoitettiin ja suoritettiin kasvotusten vapaamuotoisesti teemoja pohtien ja tarkentavia kysymyksiä kysyen. Haastattelun aikana näytettiin haastattelurungossa (liite 1) esillä olevia kuvia kommentointia varten. Kaikilta haastatelluilta ei kysytty kaikkia tarkentavia kysymyksiä, vaan teemat käytiin läpi tarpeellisin lisäkysymyksin. Haastatteluiden yhteiskesto oli 6 tuntia 36 minuuttia ja 58 sekuntia. Keskimäärin yksi haastattelu kesti tunnin ja seitsemän minuuttia.

Haastatteluäänitteet litteroitiin eli kirjoitettiin puhtaaksi käsin tietokoneella, jonka tuloksena syntyi 110 sivua A4 muotoista dokumentoitua keskusteludataa. Tämä data teemoiteltiin ja luokiteltiin teemahaastattelurungon mukaan omiin osioihinsa. Teemoitellun ja luokitellun haastatteluaineiston perusteella muodostettiin tiheä kuvaus, jossa keskustelusta poimittiin tutkimuksen kannalta merkitykselliset asiat erilliseen jäsenneltyyn dokumenttiin. Tiheän kuvauksen perusteella jäi jäljelle 26 sivua analysoitavia kommentteja. Nämä kommentit on analysoitu seuraavissa osioissa sitaattianalyysin keinoin siten, että kuvaavimpia ja keskeisimpiä haastateltujen näkökulmia on merkitty tekstin sekaan kursiivilla.

6.2 Kyberturvallisuus ja lähikäsitteet haastateltavien mukaan

Asiantuntijahaastattelurungon ensimmäisessä ja toisessa osassa (liite 1) käsiteltiin kyberturvallisuuden sekä tässä tutkimuksessa muiden keskeisten käsitteiden määrittelyitä ja täsmennettiin käsitteiden merkitykset ennen haastattelun jatkamista. Odotetusti **kyberturvallisuus**-käsitteen määrittely oli haastattelujen perusteella erittäin epäyhtenäistä ja osiltaan ristiriitaista. Asiantuntijat jakautuivat karkeasti kahteen eri näkemykseen kyberturvallisuudesta.

> *Kyberturvallisuus tarkoittaa järjestelmien luottamuksellisuutta, eheyttä ja saatavuutta. Kyberturvallisuus ja tietoturvallisuus eivät juurikaan eroa toisistaan.*

Osa asiantuntijoista ei pitänyt kyber- ja tietoturvallisuuden käsitteitä toisistaan erillisinä, vaan samaa asiaa tarkoittavina tai kyberturvallisuutta tietoturvallisuuden yhtenä osa-alueena. Näin ajattelevat asiantuntijat korostivat kyberturvallisuutta tietotekniikan tai tekno-

logian näkökulmasta – ei fyysisten toimintojen näkökulmasta. Kyberturvallisuuden erottavana tekijänä kuvattiin aktiivisen haitallisen uhan olemassaolo ja arvoketjujen puolustaminen. Toisaalta, osa asiantuntijoista piti ”kyberiä” pelkkänä markkinointiterminä.

Toinen osa haastatelluista erotti kyber- ja tietoturvallisuuden toisistaan selkeämmin. Tämä määritelmä on lähimpänä tässä tutkimuksessa käytettyä kyberturvallisuuden määritelmää.

Kyberturvallisuus on yhteiskuntaan ja mihin tahansa elämänalueisiin liittyvien ihmisten, prosessien, johtamisen ja digitaalitekniikan hallinnan turvallisuutta. Ei pelkästään tietoturvallisuutta, vaan isompi kokonaisuus.

Näissä määritelmissä korostuivat tieto- ja kyberturvallisuuden osittain päällekkäiset ja osittain erilliset ominaisuudet. Tässä kyberturvallisuuden määritelmässä tieto ei ollut ensisijainen suojattava kohde. Sen sijaan kyberturvallisuuden keskeisenä määrittäjänä nähtiin ihmisten, prosessien, organisaatioiden ja yhteiskunnan osien tietoteknisen hallitsemisen turvaaminen. Tämän näkökulman mukaisten määritelmien keskiössä oli jonkin tahon, esimerkiksi organisaation, toiminnan jatkuvuuden tai elintärkeiden toimintojen suojaaminen. Lisäksi korostettiin, että fyysistä maailmaa ohjataan kyberin avulla ja toiminnassa korostuvat valvonnan ja puolustamisen ajattelutapa. Tämä määrittely tukee tässä tutkimuksessa valittua kyberturvallisuuden määritelmää, joka on esitetty jo aiemmin käsiteluvussa 3.2.

Haastateltuja pyydettiin määrittelemään käsitteiden tilanne, tilannetieto, tilannekuva, tilanneymmärrys ja tilannetietoisuus suhteita, eroavaisuuksia ja yhteneväisyyksiä. Näiden käsitteiden osalta asiantuntijoiden näkemykset olivat melko yhteneväisiä.

Tilanne on objektiivinen totuus asioista, jotka tapahtuvat tiettynä ajanhetkenä. Se on kuin valokuva, jossa maailman meno on pysäytetty. Prosessi alkaa siitä, onko joku tapahtuma tilanne vai ei – onko tilanne päällä vai ei.

Tilanne määriteltiin haastateltavien toimesta lähes poikkeuksetta objektiiviseksi totuudeksi, joka tapahtuu tietyssä ajassa ja paikassa. Toisaalta tilanne määriteltiin myös tilaksi, josta ei vielä ole tarkkaa käsitystä. Tilannetta luonnehdittiin odottamattomaksi muutokseksi ympäristössä. Tämä määrittely on yhteneväinen tässä tutkimusraportissa käytetyn määritelmän kanssa.

Tilannetieto on tunnistettu osa tilanteen elementtejä – mitä yksittäinen ajan hetki sisältää ja mitä voimme siitä nähdä.

Asiantuntijat määrittelivät **tilannetieto**-käsitteen tilanteesta nähdyksi, havaituksi tai tunnistetuksi stimulaatioksi. Tilannetieto kuvaa mitä ja missä jotakin on tapahtunut. Yksittäinen

tilannetieto kertoo yksityiskohdan vallitsevasta tilanteesta. Yhdistämättömät eli yksittäiset tilannetiedot eivät kerro kokonaisuudesta paljoakaan, vaan ne täytyy yhdistää eli ”korrelointia” toisiinsa. Yhdistettynä tilannetiedot kattavat laajemmin tapahtuneiden asioiden olemusta. Monet asiantuntijat korostivat, että tilannetiedot eivät välttämättä kuvaa täydellistä tilannetta, vaan tilannetiedot voivat olla vääriä, puutteellisia ja johtaa harhaan. Ilman tilannetietoja ei ole kuitenkaan mahdollista saavuttaa kokonaiskäsitystä todellisesta tilanteesta. Käytännössä kybertilannekeskuksissa tilannetiedot ovat esimerkiksi lokitietoja.

Tilannekuvassa olemme menneisyyden vankeja ja katsomme tilannetta omasta näkökulmastamme subjektiivisesti. Tilannekuva muodostuu tilannetiedoista, mutta ei tarkoita ymmärrystä tilanteesta.

Tilannekuva on määritelmältään laajahko ja monimerkityksinen käsite. Tästä huolimatta asiantuntijat jakavat käsityksen tilannekuvan subjektiivisuudesta. Ihminen luo tilannekuvaa omasta näkökulmastaan ja samoista tilannetiedoista voi eri ihmisellä muodostua erilainen tilannekuva.

Tilannekuvassa tilanne osataan asettaa johonkin malliin, jonka perusteella syntyy käsitys tilanteessa tapahtuneesta. Tilannekuvaa rakennetaan CSOCissa.

Tilannekuva eroaa tilannetiedosta merkityksellisellä ja tunnistetulla sisällöllään. Tilannekuva voi asettua esimerkiksi johonkin mentaalimalliin, jossa tilannetiedoista on muodostettu merkityksiä, käsityksiä ja ne on yhdistelty tilannekuvaksi omassa mielessä. Tilannekuva ei välttämättä vastaa oikeaa objektiivista tilannetta. Yksikään haastatelluista ei ottanut esille tilannetietoisuutta ihmisryhmän yhteisenä käsityksenä vallitsevasta tilanteesta. Tässä tutkimuksessa tällaisesta tilanteesta käytetään käsitettä **jaettu tilannekuva**.

Tilanneymmärrys on johtopäätöksiä ja ymmärrystä mistä asiat ovat johtuneet ja mitä niistä seuraa. Tilanneymmärrys mahdollistaa ennaltaehkäisyä ja etukäteistä varautumista.

Asiantuntijoiden mukaan **tilanneymmärrys** on tilannekuvaa korkeampi tiedon jalostumisaste, jota harvoin täysin saavutetaan. Tilanneymmärrys tarkoittaa haastateltujen mukaan kokemusta ja kykyä hahmottaa asia oman organisaation kontekstissa kokonaisvaltaisesti. Tilanneymmärryksessä korostuvat tulevaisuuden hahmottaminen ja asioiden kehittymisen arvioiminen. Tilanneymmärryskään ei välttämättä vastaa täydellisesti objektiivista tilannetta. Tilanneymmärryksessä tärkeinä elementteinä ovat varautuminen, tilanteen jälkeen

toipuminen ja ongelmista selviytyminen. Tilanneymmärrys ei itsessään pidä sisällään toimenpiteitä asian korjaamiseksi, vaan luo edellytykset viisaiden päätösten tekemiselle. Tilanneymmärrykseen nähtiin kuuluvan myös ”järkiperustainen päätöksenteko”.

Tilannetietoisella on paljon kokemusta ja hänelle muodostuu tiedon ja kuvan lisäksi myös käsitys tilanteessa toimimisesta – silloin tein näin, sitten kävi näin.

Tilannetietoisuuden määritelmä ei haastatteluiden perusteella erottunut selkeästi aiemmin jo käsitellyistä käsitteistä. Esimerkiksi osa haastatelluista ei tunnistanut tilanneymmärryksen ja tilannetietoisuuden eroa. Yhteistä kaikille määritelmille oli, että tilannetietoisuus on ”enemmän kuin tilannekuvaa”. Lisäksi moni haastateltava korosti varautumisen merkitystä tilannetietoisuuden mahdollistamiseksi. Tilannetietoisuuden nähtiin vaativan jatkuvaa oppimista ja oivaltamista. Edellä kuvatut käsitykset ovat yhteneväisiä tässä tutkimusraportissa käytetyn tilannetietoisuuden käsitteen kanssa.

Haastatellut näkivät tilanteen, tilannetietojen, tilannekuvan, tilanneymmärryksen ja tilannetietoisuuden välillä jatkumon, jossa edellistä seuraava käsite on ”enemmän” tai ”rikastetumpi” kuin edellinen. Tämä tukee hyvin tässä tutkimuksessa käytettyä tiedon arvoketjun mallia, jossa tilanne, tilannetiedot, tilannekuva ja tilanneymmärrys muodostavat tiedon jalostumisen asteet kohti tilannetietoisuutta. Tämä on kuvattu luvussa 3.2.

6.3 Organisaation kybertilannetietoisuuden muotoutuminen

Haastattelujen kolmannessa teemassa käsiteltiin kybertilannetietoisuuden muodostumista kybertilannekuvan näkökulmasta (liite 1). Aluksi haastateltavilta kysyttiin kybertilannetietojen keräämiseen ja jakamiseen liittyviä vastuukysymyksistä (liite 1). Kybertilannetiedot ovat esimerkiksi loki- ja anturitietoja.

Haastateltujen mukaan kybertilannetiedon keräämisvastuu on ensisijaisesti kyberavaruudessa toimivalla organisaatiolla. Asiantuntijoiden mukaan tilannetietojen keräämisvastuita tulisi selkeyttää lainsäädännön avulla. Kybertilannetietojen keräämisen merkityksen arvioitiin tulevaisuudessa korostuvan ja laajenevan koskemaan yhä useampia laitteita ja palveluita. Tulevaisuudessa kybertilannetietojen kerääminen on kaikissa ratkaisuissa automaattisesti sisäänrakennettuna.

Tilannetietojen keräämistoimintaa voidaan siirtää sopimusjärjestelyin toimijoiden välillä. Esimerkiksi julkinen organisaatio voi ostaa yksityiseltä organisaatiolta tilannetietojen keräämispalvelun tilaaja-tuottaja -mallilla tai mahdollisesti koko kybertilannekeskuspalvelun. Tällöin puhutaan ostetusta kyberturvallisuuspalveluiden tarjoajasta (engl. MSSP, Managed Security Service Provider).

Yksityisten yritysten osalta sääntely tilannetietojen keräämisen laajuudesta ja vastuista vaihtelee paljon toimialakohtaisesti, joten kansainvälisen trendin mukaisesti ollaan siirtymässä toimialakohtaisiin CERT-toimintoihin (engl. Computer Emergency Response Team). Toimialakohtaiset CERT-toiminnot tuottavat tilannekuvaa tietyn toimialan – kuten energia- tai pankkitoimialan – tarpeisiin. Näissä sektorikohtaisissa ryhmissä tilannekuvaa jakavat saman toimialan organisaatiot luottamuksellisesti keskenään. Ryhmissä toimitaan vastavuoroisuusperiaatteella kybertilannetietojen ja -kuvan jakamiseksi organisaatioiden välillä.

Kaikista palveluista, sovelluksista ja laitteista pitää lähteä kybertilannetietoja erikseen käskettyyn paikkaan, jotta kybertilannekuvan muodostaminen on mahdollista.

Manuaalinen kybertilannetietojen kerääminen on harvinaisempaa, kuin automaattinen ja reaaliaikainen tietojen kokoaminen keskitettyyn lokienhallintaan tai tilannekuvajärjestelmään (SIEM). Näissä keskitetyissä paikoissa mahdollistetaan merkityksellisten päätelmien tekeminen ja tilannekuvan muodostaminen. Tätä paikkaa haastateltavat kutsuivat tuttavallisemmin SOCiksi eli kybertilannekeskukseksi.

Suppean kybertilannetiedon perusteella tehtävät toimenpiteet eivät todennäköisemmin ole oikeita, oikea-aikaisia tai oikeansuuntaisia. Toisaalta suppeallakin tiedolla on mahdollisuus osua oikeaan – sokea kanakin löytää jyvän.

Kybertilannetiedosta ei itsessään ilman jatkojalostamista ja rikastamista ole juurikaan hyötyä. Esimerkiksi teknisen tilannetiedon esittäminen yrityksen johdossa toimiville henkilöille ilman jatkojalostamista voi johtaa tilanneymmärryksen puutteeseen, kontekstin epäselvyyteen ja tapahtuman vakavuuden virhearviointiin. Kokenutkin ammattilainen voi tällöin tehdä vääriä johtopäätöksiä. Tällöin päätöksetkin ovat todennäköisemmin vääriä tai huonoja. Tilannetietojen kerääminen ei tällöin riitä, vaan tietoa on jatkojalostettava tilannetietoisuuden saavuttamiseksi.

Seuraavassa vaiheessa haastateltavilta kysyttiin kybertilannetietojen laadun: laajuuden, suppeuden tai yhtenäisyyden merkityksestä osana tilannetietoisuuden muodostamista

(liite 1). Tilannetiedon laadulla ja keräämisen laajuudella on ratkaiseva merkitys myöhemmissä tilannetietoisuuden vaiheissa. Järjestelmät, jotka eivät tuota laadukasta ja laajaa kybertilannetietoa, eivät voi tuottaa – eikä niistä voida tuottaa – kybertilannetietoisuutta myöhemmissä vaiheissa. Suppean ja vähäisen tilannetiedon ongelmana on päätösten perustuminen yksittäisiin seikkoihin, jotka eivät välttämättä pidä paikkaansa tai ovat ristiriitaisia. Suppean tilannetiedon myötä päätöksien valistumattomuus, tuurilla onnistuminen ja riski väärien toimenpiteiden toteuttamiseen kasvaa. Lisäksi suppea tilannetieto voi johtaa liian vähäisiin varautumistoimenpiteisiin suhteessa vallitsevan ympäristön uhkaan ja haavoittuvuuksiin.

Päinvastaista tilannetta eli tilannetiedon suurta määrää ei nähty ongelmana, sillä suuresta määrästä tilannetietoja voidaan tehdä varmempia johtopäätöksiä ja tietoja voidaan tarvittaessa karsia.

Jaettu tilannekuva monelta toimijalta ja eri näkökulmista muodostaa paremman ja moniulotteisemman mallin, josta voi syntyä parempi tilanneymmärrys.

Haastatteluiden kolmannen teeman toinen keskeinen osa koski kybertilannekuvan muodostumista ja jakamista eli ”jaettua tilannekuvaa” ja kybertilanneymmärrystä (liite 1). Kybertilannekuvan jakaminen tarkoittaa sekä tiedon jakamista ihmiseltä toiselle tilannekuvaa tuottavassa organisaatiossa, että tilannekuvan jakamista kybertilannekuvaa tuottavien organisaatioiden välillä. Asiantuntijat korostivat erityisesti johtajien tarvetta jaetulle tilannekuvalle oman organisaation sisällä tapahtuvista asioista. Tilannekuvan jakamista tarvitaan organisaation eri osastojen koordinoimiseen yhteisen tavoitteen saavuttamiseksi. Ilman jaettua tilannekuvaa, voidaan nykytilanne käsittää merkitykseltään eri tavoin, sillä tilannekuva on aina yhden ihmisen subjektiivinen käsitys vallitsevasta tilanteesta.

Mitä täydellisempi tilannekuva on – jaettuna paranee – sitä paremmin voidaan varautua tulevaan.

Organisaatioiden, varsinkin kybertilannekeskusten, välinen tilannekuvan jakaminen on hyödyllistä, sillä kyberuhat ovat globaaleja ja ne ilmenevät kyberavaruuden eri osissa ja eri organisaatioiden järjestelmissä eri tavoin. Asiantuntijat pitävät tärkeänä kybertilannekeskusten välisen tiedonvaihdon kehittämistä muun muassa uhkien ilmenemistavoista, ajoista ja toimintaperiaatteista. Näin voidaan varautua paremmin oman toiminnan tai edunsaajan suojaamiseen. Samalla tehdään hyökkääjien toiminnasta kannattamattomampaa ja hahmotetaan kyberavaruudessa tapahtuvien ilmiöiden laajuus ja mahdolliset yhteiskunnalliset

vaikutukset. Lisäksi organisaatioiden verkostoitumisesta ja tilannekuvan jakamisesta on hyötyä etenkin pienille organisaatioille, joilla ei ole resursseja hankkia tai tuottaa täysin omaa kybertilannekeskuspalvelua. Nämä havainnot korostavat kybertilannetietoisuuden ja varautumisen yhteyttä kybertilannekeskuksissa. Tilannetietoisuus ei itsessään riitä, vaan tarvitaan varautumissuunnitelmia ja -resursseja tilanteiden hallitsemiseksi. Edellä esitetyt havainnot tukevat tämän tutkimuksen teoreettista viitekehystä, jossa kybertilannekeskuksen toiminta perustuu sekä varautumiseen, että tilannetietoisuuden luomiseen.

Tilannetietoisuutta ja tilanneymmärrystä tarvitaan, jotta voidaan pysyä hyökkääjän kanssa samalla tasolla. Tilanteet kehittyvät kybermaailmassa nopeasti ja jos reagoimme nykytilaan, niin hyökkääjä on aina askeleen edellä.

Tilannekuvasta muodostuu tilanneymmärrystä, kun kybertilannekeskuksella on riittävät resurssit eli kokenut ja kyvykäs henkilöstö, joka osaa toimia kyberuhan vallitessa ja osaa ennakoida sekä ennaltaehkäistä tulevia uhkia haavoittuvuuksien torjumisella. Kybertilannekeskuksessa jalostuvan kyberymmärryksen ideana on pyrkiä ennakoimaan kyberuhkia ja valmistautua todennäköisimpiin kyberuhkiin resurssien käytön kannalta viisaalla tavalla. Samalla kybertilannekeskus kykenee nopeuttamaan palautumisprosessia resurssien tehokkaalla käytöllä. Asiantuntijat mainitsivat erikseen jatkuvuus- ja toipumissuunnitelmat (BCP ja DRP) keinoina parantaa tilanneymmärrystä ja tilanteenmukaisen toiminnan osuvuutta.

Tilannetietoisuus ja resurssien tietäminen on todella tärkeää: tilannekuvan jälkeen ykkösasia on yleensä käytettävissä olevien resurssien tietäminen – mitkä ovat yhteystiedot, kenelle soitetaan missäkin vaiheessa ja millä kriteereillä erityyppisiä prosesseja laukaistaan. Tämä edellyttää resurssiajattelua.

Kyberavaruudessa toimivan organisaation kybertilannetietoisuuden muodostuminen koostuu pääasiassa tiedon arvoketjun mukaisesta tiedon jalostamisesta ja sen mahdollistavista resursseista. Tämän lisäksi kybertilannetietoisuuden hyödyntämiseen tarvitaan varautumissuunnitelmien ja -kartoitusten mukaisia nopeasti käyttöön otettavia tilannevastemalleja sekä mahdollisuus luoda nopeita ratkaisuja ongelmatilanteissa. Päätöksenteon tulee olla nopeaa ja oikea-aikaista. Tilannejohtajan tulisi toimia kybertilannekeskuksessa, jossa on paras ja varhaisin tilanneymmärrys asiaan vaikuttavista seikoista. Esimerkiksi yhteyshenkilöiden suorat puhelinnumerot, tilannevasteen tuottamista hidastavien tekijöiden poistaminen ja valmiit toimintaohjeet eri skenaarioissa nopeuttavat häiriöstä palautumista.

6.4 Kyberresilienssi organisaatioissa

Teemahaastatteluiden neljännessä osassa käsiteltiin kyberresilienssiä organisationaalisesta näkökulmasta. Teemahaastattelussa keskityttiin kyberresilienssin osalta neljään aihepiiriin (liite 1): määrittelyyn, resilienssiin haitallisen tapahtuman yhteydessä, riskienhallinnan ja kyberresilienssin suhteeseen.

Tuulettimeen aina osuu ja miten siitä selviää, se on kyberresilienssiä. Kyberresilienssi vaatii jatkuvaa oppimista ja syyttelyn välttelyä.

Yksittäistä poikkeusta lukuun ottamatta asiantuntijat määrittelivät kyberresilienssin kyvyksi vastata eli torjua ja toipua uhista niiden toteutuessa. Yhden asiantuntijan mielestä kyberresilienssi koskee vain palautumista ja toipumista, mutta ei vastustuskykyä. Haastatellut korostivat harjoittelun ja jatkuvan oppimisen merkitystä kyberresilienssin parantamisessa. Hyvää kyberresilienssiä pidettiin ”kypsän” kyberavaruudessa toimivan tahon merkkinä. Kypsyydestä esimerkkinä mainittiin varajärjestelmien toteuttaminen ja siirtyminen korvaaviin toimintatapoihin elintärkeiden toimintojen turvaamiseksi, kuten käsin tehtävään paperityöhön siirtyminen tietyksi häiriöajaksi. Kyberresilienssiä määriteltiin mittarina organisaation kyvylle kestää perustason erilaisia kyberuhkia. Monissa tapauksissa kyberresilienssi rinnastettiin kyberturvallisuuden jatkuvuudenhallintaan.

Kyberresilienssiä edistetään järjestelmien priorisoinnilla, luokittelemalla pakolliset ja keskeiset järjestelmät, miettimällä vaikuttavia kyberuhkia eli miten niistä pystytään toipumaan ja palauttamaan normaalitilanne.

Kyberresilienssi nähtiin kokonaisvaltaisesti ihmisten, teknologian, prosessien ja johtamisen näkökulmasta. Esimerkiksi tietoteknisten järjestelmien tulisi olla jo hankittaessa rakennettu toipumaan nopeasti ja selviytymään erilaisista häiriöistä. Ihmisten tulisi olla koulutettuja suorittamaan palautumistoimenpiteitä ja johtamista tulisi tukea jalostetulla tilannekuvalla.

Resilienssissä on kaksi lähestymistapaa: varautuminen ja toipuminen. Molemmat ovat hyviä lähestymistapoja: halutaan estää hyökkäys kokonaan ja varmistaa haittavaikutusten vähäisyys, kun uhka toteutuu.

Asiantuntijat jakoivat kyberpoikkeaman elinkaaren ajan suhteen karkeasti kolmeen tai neljään vaiheeseen: valmistautuminen, mukautuminen, toipuminen ja sopeutuminen.

Kolmivaiheinen jaottelu sisälsi häiriötä edeltävänä ajan (ennaltaehkäisy), toimet tapahtuman aikana (hallinta) ja tapahtuman jälkeiset toimenpiteet (oppiminen). Oppivan, jatkuvasti kehittyvän ja Lean-ajattelumallia noudattavan organisaation on mahdollista palautua uhan toteutumisen jälkeen toimintotasoltaan aiempaa korkeammalle, jolloin resilienssi kasvaa. Toisaalta, asiantuntijat eivät pitäneet nykyisten suomalaisten organisaatioiden kykyä tähän kovin hyvänä ja korostivatkin ensisijaisesti toiminnan palauttamista siedettävälle tasolle alkuperäisen toimintotason parantamisen sijasta.

Tyypillisesti resilienssin taso ei parane kriisin jälkeen (se olisi ihannetilanne), sillä tyypillisessä suomalaisessa yrityksessä varautuminen on huonoa. Tällöin pienenkin poikkeaman vaikutus on lamauttava ja palautumisvaihe kestää kauan.

Kyberresilienssiä kuvaavina tekijöinä asiantuntijat korostivat **toimintotasoa** ja **kulunutta aikaa.** Tämä tukee hyvin tämän tutkimusraportin teoriapohjaa. Asiantuntijoiden mukaan toipumisvaihe on tyypillisesti mukautumisvaihetta ajallisesti pidempi. Tämä tarkoittaa, että organisaatioiden tyypillinen nopeus toipua kyberpoikkeamasta ei ole yhtä hyvä, kuin kyberhäiriöiden aikaansaaman toimintotason aleneman nopeus. Asiantuntijoiden mukaan ei ole realistista, että kyberresilienssi voisi olla tasolla, jossa häiriöillä ei olisi minkäänlaisia vaikutuksia organisaatioiden toimintaan. Tästä huolimatta vaikutukset organisaation tavoitteiden saavuttamiseksi voidaan asiantuntijoiden mukaan pyrkiä minimoimaan hyvällä kyberresilienssin tasolla. Kyberresilienssin parantaminen ei asiantuntijoiden mukaan edellytä kaikkien kyberturvallisuuden osa-alueiden parantamista, vaan toimia voidaan priorisoida riskiarvioiden perusteella kriittisimpiin toimintoihin.

Kyberresilienssi saattaa tapahtuman jälkeen jäädä pysyvästi myös alemmalle tasolle tai täysin nollaan.

Haastatteluiden analyysissä havaittiin, että tiettyjen kriittisten toimintojen menettäminen tai liian kauan jatkunut häiriö voi tarkoittaa organisaatioiden toimintaedellytysten päättymistä kokonaan. Käytännössä tämä voi tarkoittaa esimerkiksi konkurssia tai organisaation toiminnan tavoitteiden saavuttamatta jäämistä. Tämä tukee teorialuvussa esitettyjen kriittisen siedettävän häiriöajan (MTPD) ja toimintotason (MBCO) arvoja.

Riskienhallinta on strategisena keskeinen osa resilienssiä, sillä strategisen näkyvyyden puute eli huono tilannekuva johtaa epäosuviin investointipäätöksiin suojaavien järjestelmien osalta.

Kybertilannekeskustoiminta on asiantuntijoiden mukaan jatkuvaa riskienhallintaa. Riskienhallintaprosessit kybertilannekeskustoiminnan toteuttamiseksi vaihtelevat jonkin verran. Riskienhallinnan osuus korostuu erityisesti suunniteltaessa varautumista ja tehtäessä organisaation kyberympäristön riskikartoituksia. Operatiivinen kybertilannekeskustyö on asiantuntijoiden mukaan jatkuvaa riskienhallintaa ilman raskaita riskienhallintaprosesseja. Riskienhallinta ja kyberresilienssi yhdistyvät myöhempää varautumissuunnittelua varten tuotettavassa suojattavien toimintojen luokittelussa ja priorisoinnissa.

Kybertilannekeskuspalvelun tuottaminen tai ostaminen on organisaatiolle kallista ja resursseja kuluttavaa. Hyvään resilienssitasoon ei päästä välittömästi keskuksen perustamisen jälkeen, sillä kybertilannekeskuksen toiminnan kehittäminen vaatii paljon aikaa.

6.5 Organisaation kyberresilienssiin vaikuttaminen

Organisaation kyberresilienssiin voidaan vaikuttaa ennaltaehkäisyllä: ihmisiä kouluttamalla, prosesseja parantamalla, kehittämällä parempia teknisiä ratkaisuja ja johtajuutta.

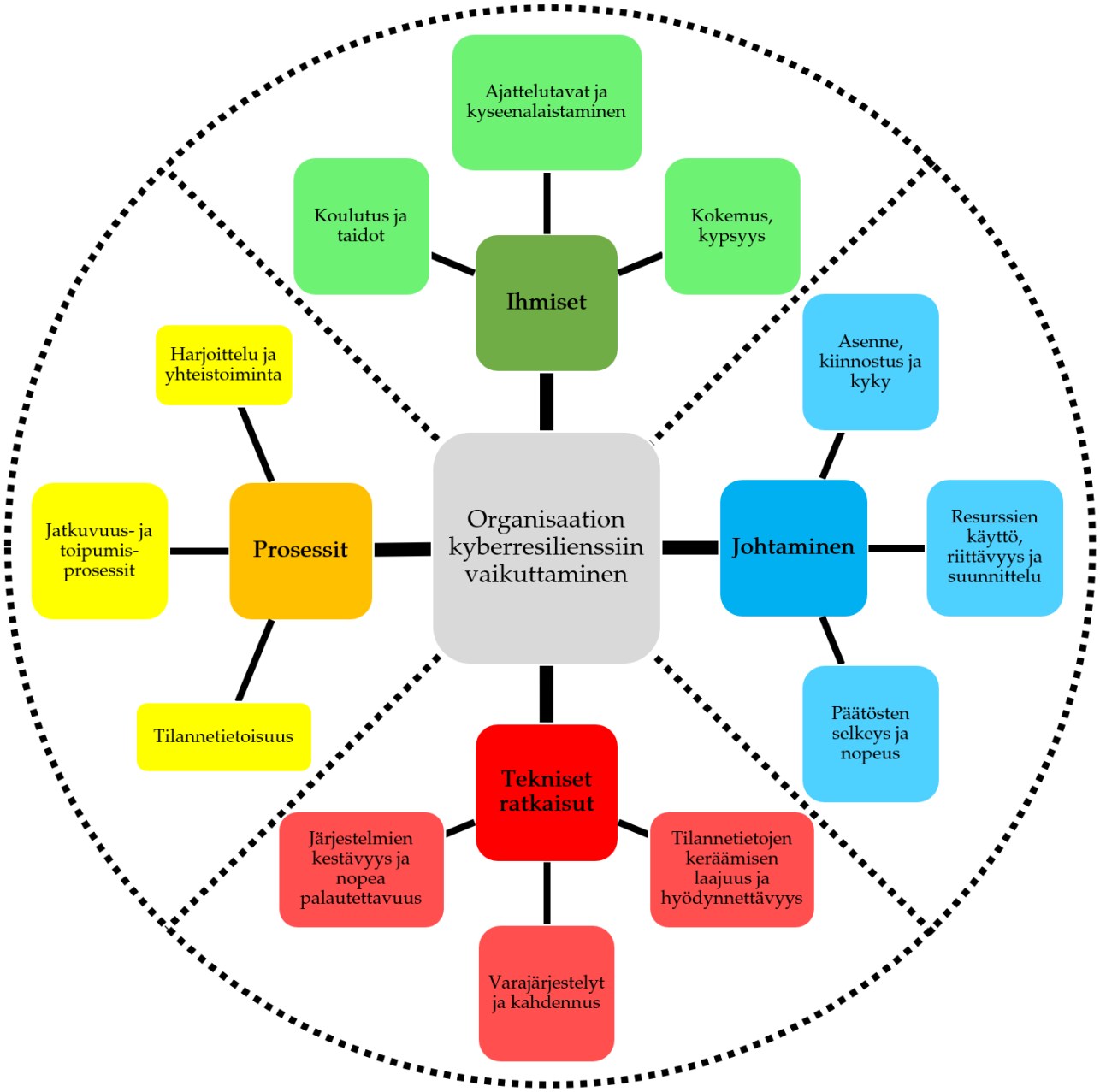
Organisaation kyberresilienssiin voidaan haastatteluiden (liite 1) perusteella vaikuttaa monin keinoin. Vaikuttamisen tavat voidaan jakaa kaikkien haastatteluiden perusteella karkeasti neljään osaan: **ihmisiin**, **johtamiseen**, **teknisiin ratkaisuihin** ja **prosesseihin**. Näistä muodostuvat tämän tutkimuksen keskeiset löydökset, joihin kybertilannekeskuksen tutkittua toimintamallia verrataan luvussa 7. Löydökset on esitetty graafisesti kuviossa 23.

Lean-ajattelutapa, jolla kyseenalaistetaan omaa toimintakulttuuria kehittää resilienssiä.

Yhtenä neljästä keskeisestä osa-alueesta ovat **ihmiset** (kuvio 23) ja ihmisten toiminnan vaikutus organisaation kyberresilienssiin. Kyberavaruudessa toimivan organisaation kyberresilienssiin vaikuttavat ihmisten koulutus ja taidot, kyberpoikkeamista ilmoittaminen ja kyberturvallisuuden perusasioiden tiedostaminen. Kyberresilienssiä parantavat toimintatapojen jatkuva kehittäminen ja kyseenalaistaminen. Organisaatiossa vallitsevalla kyberturvallisuusasioihin liittyvällä toimintakulttuurilla on merkittävä vaikutus organisaation kyberresilienssiin.

Esimerkiksi kybertuvallisuusasioista piittaamaton ajattelutapa ja sääntöjen vastaiset käytännöt johtavat huonompaan kyberresilienssiin. Omia toimintatapoja kehittävä ja kriittisesti

nykyratkaisuihin suhtautuva ajattelutapa parantaa kyberresilienssiä huomattavasti todennäköisemmin. Ihmisten kokemuksella ja hiljaisella tiedolla vaikutetaan vastatoimien nopeuteen ja tehokkuuteen häiriötilanteessa.



Kuvio 23. Organisaation kyberresilienssiin vaikuttavat neljä osa-aluetta prosessit, ihmiset, johtaminen ja tekniset ratkaisut asiantuntijahaastatteluista tehdyn analyysin perusteella.

Joissakin organisaatiossa ajatellaan, että olemalla välittämättä kyberpoikkeamista ollaan niiltä turvassa.

Toisen keskeisen organisaation kyberresilienssiin vaikuttavan osa-alueen **johtamisen** (kuvio 23) vaikutus organisaation kyberresilienssiin välittyy johtajien asenteen, kiinnostuksen ja kyvyn kautta käsitellä kyberavaruuteen liittyvää toimintaa. Kyberturvallisuusasioiden

tärkeyden ymmärtämien on keskeistä organisaation toiminnan jatkuvuuden ja häiriöistä toipumisen kannalta. Tietämättömyys, välinpitämättömyys ja ylimmän johdon piittaamattomat asenteet johtavat todennäköisemmin huonoon organisaation kyberresilienssiin. Kyberturvallisuusasioista kiinnostunut johtaja parantaa kyberresilienssiä todennäköisemmin. Johtajalta vaaditaan riittävää osaamista, kykyä ja taitoja kyberturvallisuusasioiden ymmärtämiseksi.

Organisaation kyberresilienssiin voidaan vaikuttaa vakuuttamalla liiketoimintajohto resurssien tarpeesta. Ongelmana on turvallisuuden kaksisuuntaisuus: kun turvallisuudesta huolehtivat tekevät työnsä hyvin, näyttää työn tarve laskeneen. Kun turvallisuudesta huolehtivien resursseja lasketaan, työn tarve kasvaa turvattomuuden lisääntyessä. Jatkuva vuoristorata luo haasteen tasaiselle kehittämiselle ja resurssivirralle.

Ylimmän johdon ymmärrys tasaisen ja ennustettavan resurssivirran sekä kyberresilienssin parantamisen välisestä suhteesta on tärkeää. Kyberturvallisuuteen panostettavien resurssien tulisi olla pitkäaikaisia ja suunnitelmallisia. Kyberresilienssin parantamiseen tulee varata resursseja riittävästi siten, että vakavistakin häiriöistä toipuminen on mahdollista. Resurssien vähyys johtaa organisaation toiminnan jatkuvuuteen liittyvien riskien kasvamiseen. Toisaalta liian kallis ja paljon resursseja kuluttava varautuminen voi johtaa organisaation muiden tavoitteiden saavuttamatta jäämiseen. Johtotason päätöksenteon selkeydellä ja oikea-aikaisuudella on merkittävää vaikutusta organisaation kyberresilienssiin. Päätöksenteon kankeus ja hitaus johtaa todennäköisemmin resilienssin huonontumiseen.

Organisaation kyberresilienssiin voidaan vaikuttaa tekemällä käytetystä järjestelmästä kestävämpi tai vikasietoisuuden lisäämisen ollessa mahdotonta ylläpitämällä varajärjestelmää.

Kolmas organisaation kyberresilienssiin vaikuttava osa-alue on **tekniset ratkaisut** (kuvio 23). Kyberavaruudessa teknisten ratkaisuiden toimivuus on ratkaisevassa osassa resilienssin kannalta. Kyberresilienssin olemassaolon edellytyksenä ovat kyberavaruuden havainnointi- ja hallintakyvyt.

Havainnointikyvyn osalta kyberresilienssiin vaikuttavat erilaisten tilannetietojen, lokituksen, anturitiedon ja muun uutisvirran laajuus ja laatu. Ilman järjestelmien tuottamia tietoja ei ole mahdollista aloittaa korjaavia toimenpiteitäkään. Tilannetietoja tulisi pystyä hyödyntämään automaattisesti ja jatkojalostamaan tarpeen mukaan.

Hallintakyvyn osalta kyberresilienssiin vaikuttavat järjestelmän kestävyys ja vikasietoisuus. Varajärjestelmien ylläpitäminen elintärkeiden toimintojen osalta parantaa resilienssiä, mutta on suuressa mittakaavassa kallista. Lähtökohtaisesti kyberavaruudessa käytettävien järjestelmien tulisi olla sellaisia, että ne sietävät jatkuvasti erilaisia perustason hyökkäyksiä ja häiriöitä sekä pystyvät toipumaan tarvittaessa nopeasti. Tätä varten järjestelmien suunnitteluun ja hallintakäyttöliittymien helppokäyttöisyyteen on kiinnitettävä huomiota.

Organisaation kyberresilienssiin voidaan vaikuttaa negatiivisesti huonolla tai olemattomalla kybertilannekuvan luomisella (ei tiedetä ongelmista).

Neljäs organisaation kyberresilienssiin vaikuttava teema on **prosessit** (kuvio 23). Haastatteluissa korostuivat erityisesti tilannetietoisuuden ja siihen pääsemisen (prosessin) tärkeys kyberresilienssiin vaikutettaessa. Ilman tilannetietoisuutta on käytännössä mahdoton toipua kyberhäiriöistä nopeasti ja toisaalta ymmärtää, mistä häiriö ylipäätään johtuu. Varautumisen eli jatkuvuus- ja toipumissuunnitelmien toteuttamista pidettiin kaiken kyberresilienssiä parantavan toiminnan edellytyksenä.

Harjoittelulla ja kouluttamisella voidaan vaikuttaa kyberresilienssiin. Harjoittelua pitäisi olla vähintään vuosittain tai puolivuosittain.

Harjoitustoiminnan avulla on mahdollista tunnistaa organisaation kybertoiminnan kannalta keskeisten järjestelmien tärkeysjärjestys, joka mahdollistaa elintärkeiden toimintojen palauttamisen priorisoimisen häiriötilanteessa. Samalla kehitetään toimintavalmiutta, joka vaikuttaa häiriöstä toipumisen nopeuteen. Harjoittelemalla yhteistyössä muiden organisaatioiden kanssa on mahdollista löytää päällekkäisiä toimintoja eli synergiaetuja, jotka voivat tukea toisiaan häiriötilanteissa.

Yhtä kaikki, keskeisiä kyberresilienssiin vaikuttavia tekijöitä ovat (kuvio 23) säännöllinen harjoittelu, ihmisten kouluttaminen, resurssien riittävyyden varmistaminen, kybertilannekeskustoiminnan jatkuva kehittäminen, omien toimintatapojen kyseenalaistaminen, tilannetietoisuuden parantaminen, varautumissuunnittelu, johtajien asenteen, ammattitaidon ja työpaikkakulttuurin kehittäminen sekä automaattisten teknisten ratkaisujen luominen häiriötilanteita varten.

6.6 Kybertilannekeskuksen vaikutus organisaation kyber-resilienssiin

Teemahaastatteluiden viidennessä osassa (liite 1) käsiteltiin kybertilannekeskusta ja kybertilannekeskuksen vaikutusta organisaation kyberresilienssiin. Suurin osa kybertilannekeskuksen operatiivisesta käytännön toiminnasta on käsitelty jo aiemmin tutkimusraportin empiriaosuudessa, jossa on hyödynnetty asiantuntijahaastatteluilla saatuja tuloksia. Tästä syystä tässä alaluvussa käsitellään kybertilannekeskuksen käytännön toimintaa vain tarpeellisin osin.

Kybertilannekeskuksen tehtävä on organisaation kyberresilienssin operatiivinen ylläpitotehtävä: asioiden pieleen meneminen johtaa toipumisprosessiin, joka on harjoiteltu, dokumentoitu, suunniteltu, resursoitu, verkottunut ja koordinoitu.

Asiantuntijoiden mukaan kybertilannekeskuksen tehtävänä on mahdollisimman reaaliaikaisen ja hyvän kybertilannekuvan tuottaminen, kyberpoikkeamatiedon kerääminen, poikkeamien tunnistaminen ja resurssien kohdistaminen tehokkaasti poikkeaman vaikutusten vähentämiseksi tai poistamiseksi. Kybertilannekeskuksen tehtävänä on suojata organisaation toimintaa mukautuen ympäristön ja uhkatilanteiden muutoksiin resilientisti. Kybertilannekeskuksen tehtävänä on lisäksi jakaa ja välittää tilannekuvaa esimerkiksi edunsaajaorganisaation johdolle.

Kybertilannekeskus tuottaa kybertilannekuvaa, joka on osaltaan resilienssin työkalu: sitä käytetään varautumiseen ja toipumiseen työkaluna. Sen avulla tiedetään jotakin käsillä olevasta tilanteesta ja voidaan reagoida siihen.

Kybertilannekeskus tuottaa jokaisen haastatellun asiantuntijan mukaan tilannekuvaa ja resurssitietämystä keinoista, joilla mahdolliseen poikkeamaan voidaan vastata. Keskuksen tuottamat tilannekuvatuotteet voidaan rinnastaa tiedusteluorganisaatioiden tuottamiin tiedustelutuotteisiin. Keskuksen tilannekuvatuotteista on hyötyä esimerkiksi organisaation johdolle päätöksenteossa ja operatiivisessa kyberturvallisuuden päivittäisessä hallinnassa. Kybertilannekeskus voi lisäksi tuottaa varmuuden tunteen poikkeamiin puuttumisesta.

Kybertilannekeskus tuottaa toipumista poikkeamanhallintasuunnitelman mukaisesti. SOCin toiminta tulisi näkyä järjestelmien saatavuudessa ja jatkuvuudessa. Tällöin kybertilannekeskus tuottaa resilienssiä.

Tilannekuvan ja tietämyksen lisäksi kybertilannekeskus kehittää järjestelmien saatavuutta ja jatkuvuutta, jolloin kybertilannekeskus vaikuttaa suoraan organisaation kyberresilienssiin.

Kybertilannekeskus seuraa organisaation kyberympäristöä, SOCiin liitettyjä järjestelmiä ja laitteita sekä tunnistaa organisaation liiketoimintaan kuuluvaa normaalia ja epänormaalia jatkuvaa kybertoimintaa. Poikkeamia analysoidaan tarkemmin ja niiden perusteella tehdään päätökset toimenpiteistä.

Kybertilannekeskusten hyötyjä ovat muun muassa häiriöiden ennaltaehkäisykyvyn parantuminen, jatkuva tilannekuvan saaminen, selkeytetyt päätöksentekorakenteet kriisitilanteessa ja päätösten onnistumistodennäköisyyden parantaminen. Lisäksi osalle toimialoista kybertilannekeskustoiminta ja siihen liittyvä varautuminen voivat olla pakollinen toiminnan edellytys, esimerkiksi lainsäädännön takia.

SOC-toiminta maksaa paljon.

Kybertilannekeskustoiminnan haittapuolena on suuri resurssien kulutus. Kyberturvallisuuden ”ulkoistaminen” kybertilannekeskukselle – ilman valmiutta oman toiminnan muutoksiin – voi joissain tapauksissa johtaa kyberresilienssin huononemiseen. Kybertilannekeskus ei asiantuntijoiden mukaan ole ratkaisu ongelmiin, vaan työkalu ongelmien käsittelemiseksi.

Hyökkäysten taajuuteen tai ulkopuoliseen tekijään ei voida vaikuttaa.

Haastattelujen perusteella kybertilannekeskustoiminnalla ei voida vaikuttaa tahoihin, jotka tekevät kyberhyökkäyksiä: kyberaktivisteihin, kyberrikollisiin tai muihin häiriöitä aiheuttaviin tekijöihin (kuten luonnonilmiöihin). Tästä huolimatta hyvällä kyberturvallisuuden tasolla voidaan vähentää kyberrikollisten halua hyökätä hyvin varautunutta asiakasorganisaatiota kohtaan ja suurentaa kiinnijäämisriskiä. Toisaalta hyvä suojaustaso voi tarjota haasteen aloittelevalle hakkerille ja motivoida hyökkäyksiin. Näin ollen ulkopuolisen tahon toimintaan ei kybertilannekeskuksella voida suoraan vaikuttaa.

6.6.1 Ihmiset

Kybertilannekeskuksissa työskentelevät asiantuntijat ovat kyberturvallisuusalan erikoisosaajia, jotka ovat tyypillisesti korkeasti koulutettuja ja omaavat hyvät tekniset taidot. Kybertilannekeskuksen työntekijöiden vuorovaikutustaidot ja kyky ryhmätoimintaan parantavat tilannekuva- ja vastetoiminnan nopeutta ja osuvuutta.

Parhaassa tapauksessa opitaan ja parannetaan organisaation toimintaa koettujen poikkeamatilanteiden perusteella.

Kybertilannekeskuksen työntekijöiden joukossa on tyypillisesti osaajia, jotka voivat opastaa ja kouluttaa edunsaajaorganisaation työntekijöitä turvallisempiin toimintatapoihin. Monet kyberuhat kohdistuvat edunsaajaorganisaation työntekijöihin ja johtoportaaseen, jolloin mahdollisia väärinkäytösten onnistumistodennäköisyyttä voidaan pienentää.

Kybertilannekeskuksen päivittäisen toiminnan tasoa voidaan arvioida maturiteettitasolla eli kypsyystasolla. Maturiteettitasoon vaikuttavat laitteiston taso, henkilöstön osaaminen ja kokemus, henkilöstövaihtuvuuden sujuvuus (perehdyttäminen, mentorointi ja organisointi), henkilöstön sitoutuminen, työyhteisön toimivuus ja järjestelmien kytkeminen toisiinsa.

Tyypillisesti kybertilannekeskuksissa työskentelee sekä kokemattomampia, että hyvin kokeneita työntekijöitä. Kokeneemmat työntekijät ratkaisevat vaikeimmat tapaukset ja kokemattomammat oppivat kokeneemmilta. Mitä kokeneempia ja osaavampia työntekijöitä kybertilannekeskuksessa on, sitä todennäköisemmin häiriöistä toipuminen on nopeaa ja tehokasta. Tyypillisesti osaavien ja kokeneiden työntekijöiden palkkaaminen on kuitenkin kallista ja löytäminen haastavaa.

6.6.2 Johtaminen

Kybertilannekeskustoiminta on koordinoitua ja johdettua toimintaa, jonka myötä selkeytetään päätöksenteon rakenteita, sovitaan toimivaltuuksista ja erilaisten toipumisprosessien kriteereistä. Näistä sopiminen voidaan tehdä esimerkiksi SLA-sopimuksessa (engl. Service Level Agreement) eli palvelutasosopimuksessa edunsaajaorganisaation ja kybertilannekeskuksen välillä. Tyypillisesti kybertilannekeskuksilla on toimivaltuus määritellyn laajuisiin toimenpiteisiin itsenäisesti. Vain kaikista laajimmat toimenpiteet tulee hyväksyttää edunsaajaorganisaation ylimmässä johdossa. Näin päätöksenteko on hajautetumpaa, nopeampaa ja vastuukysymykset selkeitä. Tämä parantaa kyberhäiriöstä palautumisnopeutta ja resurssien käytön tehokkuutta.

Johto saa raportoinnin kautta kuvan omasta kyberympäristöstään: poikkeamien frekvenssit ja toimenpiteiden vaikutus poikkeamien määrään. Toimenpiteet voidaan kohdentaa oikein ja selvittää mikä toimenpide vaikuttaa resilienssiin.

Kybertilannekeskuksen koordinoidessa ja kehittäessä kybertilannekuvaa, voidaan käytössä olevia resursseja kohdentaa tilannetietoisuuden parantamisen kannalta tärkeisiin kohteisiin. Resurssien käyttämien on tällöin tehokkaampaa ja parantaa kyberresilienssiä.

Kybertilannekeskustoiminnan organisoinnissa tulee välttää tilannetta, jossa kybertilannekeskus voi vaikuttaa omien resurssiensa suuruuteen. Kybertilannekeskuksen resursseista tulee päättää edunsaajaorganisaation tarpeiden mukaisesti. Kybertilannekeskus voi kuitenkin tuottaa monipuolisia tilannekuvatuotteita edunsaajaorganisaation johdolle kyberavaruuden muutoksista. Näin toimittaessa kybertilannekeskus voi perustella resurssitarpeitaan ja hyödyttää ylintä johtoa liiketoiminnan kehittämisessä. Jos resurssit kybertilannekeskukselle eivät ole suunnitelmalliset ja jatkuvat, voi keskuksen toiminnasta tulla tempoilevaa, kallista ja tehotonta.

Edunsaajaorganisaation ylimmän johdon asenne kyberturvallisuusasioita kohtaan on merkittävä tekijä kyberresilienssin kannalta, sillä häiriöihin varautumiseen ja häiriönaikaiseen toimintaan tarkoitetut resursointipäätökset tehdään ylimmän johdon toimesta.

6.6.3 Tekniset ratkaisut

Kybertilannekuvaa tulisi kerätä laajasti kaikenlaisista laitteistoista, joissa kybertilannetietojen keräämismahdollisuus olisi sisäänrakennettuna.

Kybertilannekeskuksen ydintoimintaa ovat tilannetietojen keskitetty kerääminen ja synteesi. Tilannetietojen keräämistä kehitetään ja ylläpidetään jatkuvasti, jolloin tilannetietojen kattavuus ja laatu paranevat ajan myötä. Tämä parantaa muun muassa häiriötilanteesta toipumisen nopeutta. Tilannetietojen keräämistä ja tilannekuvan luomista voidaan automatisoida, joka nopeuttaa toimintaa entisestään. Nämä tekijät parantavat edunsaajaorganisaation kyberresilienssiä.

Kybertilannekeskus seuraa hälytyksiä ja selvittää niiden taustoja sekä automatisoi ja sujuvoittaa prosessejaan tehden itsensä työttömäksi, jotta uusiin uhkiin voidaan keskittyä.

Kybertilannekeskus voi antaa oma lausuntonsa uusien tietojärjestelmähankintojen kyberturvallisuudesta ja tilannekuvatoimintaa tukevista ominaisuuksista. Näin voidaan hankkia tietojärjestelmiä, joiden häiriövastustuskyky on jo sisäänrakennettuna parempi ja joita voidaan korvata tarvittaessa varajärjestelmillä. Tämä parantaa organisaation kyberresilienssiä.

Tietoteknisen kehityksen nopeuden ja uusien uhkien kehittymisen vuoksi teknisten ratkaisuiden tulee olla jatkuvasti ajantasaisia ja turvallisia käyttää. Vuosittainen ”katselmus” teknisten laitteiden kunnosta ja päivitystarpeesta on nykyisessä uhkaympäristössä riittämätön toimintatapa. Kybertilannekeskus voi reagoida välittömästi turvallisuuspäivitysten julkaisuiden asentamiseen ja havaittujen haavoittuvuuksien korjaamiseen.

6.6.4 Prosessit

Jos olet sokea, kävelet päin seiniä. Sama toimii kybermaailmassa.

Kybertilannekeskus vaikuttaa organisaation kyberresilienssiin erityisesti prosessien kehittämisen avulla ja toimii organisaation mahdollisuutena tietää ja tuntea, mitä omassa kyberympäristössä tapahtuu. Kybertilannekeskus on kuin hermokeskus, johon aistielimistä eli antureista tulee tilannetietoa. Ilman ajantasaista tilannekuvaa, ei vastatoimia voitaisi tehdä ja varautuminenkin olisi todennäköisemmin vääränlaista tai -tasoista.

Kyberresilienssiin voidaan vaikuttaa suunnittelun ja varautumisen myötä tunnistetuilla toimenpiteillä: poikkeamatilanteiden kokonaan estäminen, vaikutuksen vähentäminen ja palautumisvaiheen nopeuttaminen.

Kybertilannekeskuksen jatkuvana tehtävänä on varautumistoiminnan kehittäminen. Ajantasaiset, dokumentoidut ja käytännön toimintaan jalkautetut jatkuvuus- ja toipumissuunnitelmat mahdollistavat tositilanteessa järjestelmälliset, tehokkaat ja täsmälliset keinot kyberresilienssin ylläpitoon.

Kun verkostoituu ja tuntee toiset, niin apuakin saa paremmin.

Jatkuvalla omatoimisella harjoittelulla voidaan löytää edunsaajaorganisaation haavoittuvuuksia ennen, kuin niitä käytetään haitallisiin tarkoituksiin. Samalla voidaan harjoitella yhteistyötä viranomaisten ja muiden kyberturvallisuusalan toimijoiden kanssa ja jakaa tietoa viimeisimmistä kyberuhista. Näin toimittaessa voidaan sujuvoittaa mukautumis- ja toipumisvaiheita.

7 TUTKIMUSTULOKSET

Tässä luvussa tarkastellaan tutkimuksen tuloksia, arvioidaan kriittisesti suhdetta muihin tutkimuksiin ja vastataan tutkimuskysymykseen. Lisäksi tarkastellaan aiemmasta tutkimuskirjallisuudesta sovelletun teoriataustan ja empiirisen aineistonhankinnan avulla saatujen tulosten yhtenevyyttä ja eroavaisuuksia.

7.1 Teoreettisen viitekehyksen ja empirian yhteensopivuus

Tämän tutkimuksen teoreettisen pohjan muodostaa tarkasti valittu teoreettisten mallien kokoelma, jonka avulla voidaan teoreettisesti selittää ja tutkia kybertilannekeskuksen vaikutuksia organisaation kyberresilienssiin. Teoriakokoelman ylätasolla on järjestelmäteoreettiseen paradigmaan kuuluva järjestelmäteoria, joka kuvaa kaikille järjestelmille yhteisiä ominaisuuksia (luku 4.2.1). Järjestelmäteorian piiriin kuuluvista monista teoreettisista malleista kybertilannetietoisuuden luonnetta kuvasi sopivimmin järjestelmien kompleksisuuden ja tietoisuuden suhdetta kuvaava hierarkiamalli (luku 4.2.2). Edellisen lisäksi kybertilannekeskuksen toimintaperiaatteita yleisellä tasolla kuvasi parhaiten kybernetiikan mukainen teoreettinen järjestelmämalli, joka ei sellaisenaan ollut riittävä tutkimuskysymykseen vastaamisen kannalta (luku 4.2.3). Valmiin kybertilannekeskuksen toimintaa kuvaavan teoriamallin puuttuessa muodostettiin erillinen kybertilannekeskuksen resilienssimalli, jonka perusteella voitiin tarkastella teoreettisesti tekijöitä, jotka vaikuttavat edunsaajaorganisaation kyberresilienssiin (luku 4.3). Seuraavaksi tarkastellaan tutkimusraportin teoreettisen viitekehyksen sopivuutta empiirisiin tuloksiin tutkimuskysymyksen näkökulmasta.

Järjestelmäteoria kuvaa jokaiselle järjestelmälle yhteisiä ominaisuuksia. Evoluution myötä ihmiselle on kehittynyt aistit, joiden avulla voidaan havaita fyysisen ympäristön muutoksia ja tarvittaessa reagoida muutoksiin selviytymisen ja kehittymisen edellyttämällä tavalla. Järjestelmäteorian mukaan jokainen järjestelmä, kuten ihminen tai organisaatio, pyrkii tavoitehakuisesti tasapainotilaan säätelemällä itseään, rajojaan ja kasvuaan. Järjestelmät toimivat kokonaisvaltaisesti kehittäen rakenteitaan ja vastaten mukautuvasti ympäristön muutoksiin. Järjestelmien toiminnan sääntely perustuu tietoisuuteen ympäristössä ja itsessä tapahtuvista muutoksista aistien välityksellä.

Monien nykyorganisaatioiden toiminta on kytkeytynyt olennaisesti kyberavaruuteen muun muassa digitalisaation myötä. Järjestelmäteoria kuvaa monipuolisesti ominaisuuksia, joita kyberavaruudessa ja fyysisessä maailmassa toimivilla organisaatioilla on ja sopii siksi tämän tutkimuksen teoreettiseksi ylätason viitekehykseksi hyvin. Järjestelmäteorian rooli tässä tutkimuksessa on kuvata millaisia tutkimuskysymyksessä mainitut organisaatiot luonteeltaan ovat. Järjestelmäteoria mahdollistaa organisaatioiden resilienssin tutkimuksen, sillä keskeisenä organisaation ominaisuutena on teorian mukaan mukautuminen ympäristön muutoksiin. Tutkimusaineiston perusteella löydetyt monipuoliset organisaation kyberresilienssiin vaikuttavat tekijät eli ihmiset, johtaminen, prosessit ja tekniset ratkaisut kytkeytyvät järjestelmäteoriaan selittämällä kyberavaruudessa toimivan organisaation ominaisuuksia.

Keinotekoisessa datasta, tietoliikenteestä, ohjelmistoista ja laitteista muodostuvassa kyberavaruudessa laitteet suorittavat käskyjä ja toimintoja ihmisten määrittelemällä tavalla. Osa laitteista kykenee jopa oppimaan virheistään ja parantamaan toimintatapojaan. Tästä huolimatta ihminen ei ole toistaiseksi löytänyt keinoa ohjelmistoille ja laitteille rakennettavalle tietoisuudelle, joka yltäisi lähellekään ihmisen tietoisuuden kompleksisuutta. Tässä tutkimuksessa järjestelmäteorian johdannaisena esitetty **järjestelmien kompleksisuuden ja tilannetietoisuuden suhdetta kuvaava hierarkiamalli** kuvaa karkeasti tasoja, joiden mukaan tietoisuutta on olemassa.

Nykyiset koneet ja laitteet eivät yllä ihmisten tietoisuuden tasolle. Tästä syystä ilman ihmisten tai organisaatioiden osallisuutta ei voi muodostua tilannetietoisuutta. Biteistä muodostuvaa kyberavaruutta ihminen ei kykene aistimaan omilla evoluution pohjalta kehittyneillä fyysiseen maailmaan tarkoitetuilla aistielimillään, jolloin tietoisuus muutoksista ja niiden korjaamiseen vaadittavista toimista jää kyberavaruuden osalta toteuttamatta ilman erillisratkaisuja. Tässä esitetty teoreettinen malli soveltuu hyvin selittämään ihmisen osallisuuden tarpeen kybertilannetietoisuuden muodostamiseksi. Ilman erityistä tieteellistä ajattelua on mahdollista syntyä käsitys, että kybertilannekeskuksessa tuotetaan tilannetietoisuutta ihmisestä riippumatta. Tämä ei kuitenkaan vielä nykyään ole mahdollista haastatteluissa saatujen tulosten tai teoreettisten mallien mukaan. Ihmisen rooli kybertilannetietoisuuden luomisessa onkin keskeinen ja erottamaton.

Kyberavaruuden ongelmien havaitsemiseksi tarvitaan keinotekoisia aistielimiä, aistitasoja ja hermokeskuksia, jotka vastaanottavat kyberavaruuden ärsykkeitä ja muuntavat ne ihmisen aistittavaan muotoon. Käytännössä nämä aistielimet ovat teknisiä antureita, joiden havaitsemat ärsykkeet siirretään keskitettyyn järjestelmään tilannetietojen yhdistämistä varten. Ilman teknisiä ratkaisuja mikään edellä oleva ei olisi mahdollista. Tästä johtuen kybertilannetietoisuuden luomiseksi tarvitaan sekä ihmisiä, että teknisiä ratkaisuja.

Tekniset ratkaisut mahdollistavat ja helpottavat kybertilannekuvan kehittymistä, joka yhdistettynä ihmisen omaan aiempaan kokemukseen mahdollistaa tilanneymmärryksen syntymisen. Ihminen voi tällöin tehdä viisaan, punnitun ja oikea-aikaisen päätöksen tarvittavista toimista, joilla vaikutetaan kyberavaruuteen tietoteknisten laitteiden välityksellä. Toimien vaikutusta voidaan tarkastella kyberympäristöstä kybertilannekeskuksen avulla saatavan palautteen avulla.

Edellä kuvattu kybertilannekeskuksen empiirinen toimintaperiaate noudattelee tässä tutkimuksessa sovellettua **kyberneettisen järjestelmän teoreettista mallia**. Kyberneettisessä järjestelmässä ärsyke vaikuttaa vastaanottimeen, joka mahdollistaa päätöksenteon ja vaikutuselimen ohjaamisen oikeanlaisen tilannevasteen aikaansaamiseksi. Järjestelmäteorian täsmennyksenä kybernetiikka soveltuu hyvin kyberavaruudessa toimivan organisaation toimintaperiaatteiden kuvaamiseen ja vastaa hyvin empiriaosuuden havaintoja kybertilannekeskuksen toiminnasta.

Tämän tutkimuksen teoriaosuuden tärkeimmän osan muodostaa **kybertilannekeskuksen resilienssimalli**, joka pohjautuu järjestelmäteorian henkeä noudattaviin toisistaan alun perin erillisiin teoreettisiin malleihin ja resilienssitutkimuksen perusperiaatteisiin. Tutkimusartikkeleiden mukaiset mallit kuvaavat eri näkökulmista elementtejä, joita tutkimuskysymykseen vastaamiseen tarvitaan. Artikkelien mukaiset mallit yhdistettiin yhdeksi kybertilannekeskusta kuvaavaksi kokonaisuudeksi ja mallin toimivuus varmistettiin empiriaosuudella sekä tutkimushaastatteluiden analyysin tuloksilla, jotka tukevat hyvin mallin käyttöä osana tätä tutkimusta. Tämä ilmenee tutkimuskysymyksen vastauksesta.

7.2 Tutkimuskysymyksen vastaus ja tulokset

Teoriataustan eli kybertilannekeskuksen resilienssimallin (luku 4.3, kuvio 21) mukaan kybertilannekeskus vaikuttaa organisaation kyberresilienssiin kahdella tavalla: **tilannetietoisuuden** ja **varautumisen** kautta. Organisaation kyberresilienssiin vaikuttavat lisäksi **edunsaajaorganisaation ominaisuudet** eli koko, tavoitteet, sääntely, kompleksisuus, erikoistuminen, päätöksenteko ja tehokkuus kyberavaruuden näkökulmasta. Lisäksi organisaation kyberresilienssiin vaikuttavat **kyberuhan ominaisuudet**, kuten voimakkuus, kesto ja kohdentuminen.

Kybertilannekeskuksen **tilannetietoisuustoiminnon** (luku 4.3, kuvio 21) vaikutus kyberresilienssiin koostuu tilanteen muutoksen havaitsemiskyvystä, tilannetietojen muuntamisesta merkitykselliseksi tilannekuvaksi ja tilanteen kehittymisen ymmärtämisestä kokemukseen, taitoihin ja kykyyn pohjautuen. Lisäksi tilannetietoisuuteen kuuluu viisaiden ja oikea-aikaisten päätösten tekeminen tilanteen korjaamiseksi.

Kybertilannekeskuksen **varautumistoiminnon** (luku 4.3, kuvio 21) vaikutus kyberresilienssiin koostuu jatkuvuussuunnitelman (BCP) ja toipumissuunnitelman (DRP) mukaisista toimenpiteistä. Jatkuvuussuunnitelmalla vaikutetaan organisaation häiriöiden vastustuskykyyn ja toimintojen korvattavuuteen mukautumishetkellä välittömästi uhan toteutuessa. Toipumissuunnitelmalla puolestaan vaikutetaan häiriön vasteaikaan eli toipumisen aloittamisaikaan ja resurssien tehokkaaseen käyttöön eli palautumisen nopeuteen.

Haastatteluaineiston perusteella organisaation kyberresilienssiin vaikuttavia osa-alueita ovat tekniset ratkaisut, prosessit, ihmiset ja johtaminen (kuvio 23).

Kybertilannekeskuksessa tilanteen muutoksen havaitsemiskyky vaatii hyviä **teknisiä** ratkaisuja. Tilannetietojen muuntaminen merkitykselliseksi tilannekuvaksi vaatii toimivia tilannekuvan luomisen **prosesseja**. Tilanteen kehittymisen ymmärtäminen kokemukseen, taitoihin ja kykyyn pohjautuen edellyttää osaavia ja koulutettuja **ihmisiä**. Viisaiden ja oikeiden päätösten tekeminen tilanteiden korjaamiseksi vaatii hyvää ja täsmällistä **johtajuutta**.

Kyberavaruuden muutoksien varautumisen perustan muodostavat vastustuskyky, korvattavuus, nopeus ja tehokas resurssien käyttö. Ne edellyttävät hyviä teknisiä varautumisen ratkaisuja, hiottuja jatkuvuus- ja toipumisprosesseja, kokeneita ja taitavia ihmisiä nopean

palautumisen aloittamiseksi ja hyvää johtajuutta resurssien kohdistamiseksi palautumisen nopeuttamiseksi.

7.2.1 Kybertilannekeskuksen vaikutus organisaation teknisiin ratkaisuihin

Tekniset ratkaisut vaikuttava organisaation kyberresilienssiin (1) tilannetietojen keräämisen laajuuden ja hyödynnettävyyden kautta, (2) varajärjestelyiden ja kahdennuksen avulla ja (3) järjestelmien kestävyyden sekä nopean palautettavuuden kautta (kuvio 23).

1. Kybertilannekeskuksessa kehitetään ja parannetaan antureiden, lokilähteiden ja edunsaajaorganisaation ulkopuolisten tilannetietolähteiden kattavuutta. Tilannetietoja kerätään keskittäviin SIEM-järjestelmiin, jotka parantavat tilannetietojen hyödynnettävyyttä. Muita mahdollisia ratkaisuja ovat esimerkiksi palomuurit, tunkeutumisen estämis- ja havaitsemisjärjestelmät sekä yhteydenottopiste, jonne edunsaajaorganisaation ihmiset voivat kertoa havainnoistaan kybertuvallisuusasioihin liittyen.
2. Kybertilannekeskus testaa varajärjestelmien toimivuutta ja kohdentaa resursseja kaikista tärkeimpien kohteiden suojaamiseen. Varajärjestelmiä päivitetään tarpeellisilta osin ja mahdollisia lisätarpeita kartoitetaan jatkuvasti.
3. Lisäksi annetaan konsultointiapua järjestelmähankintojen kyberturvallisuusasioihin ja olemassa olevien järjestelmien kyberturvallisuuden parantamiseksi liittyviin toimenpiteisiin. Jatkuvassa käytössä olevien järjestelmien päivityksien ajantasaisuutta seurataan ja häiriöstä palautumisen toimenpiteitä automatisoidaan nopean tilannevasteen takaamiseksi.

7.2.2 Kybertilannekeskuksen vaikutus organisaation prosesseihin

Prosessit vaikuttavat organisaation kyberresilienssiin (1) harjoittelun ja yhteistoiminnan avulla, (2) jatkuvuus- ja toipumissuunnitelmien mukaisten prosessien avulla ja (3) tilannetietoisuusprosessilla (kuvio 23).

1. Kybertilannekeskuksen tehtäviin kuuluu aktiivinen harjoittelu mahdollisten poikkeus- ja häiriötilanteiden varalle. Harjoittelulla parannetaan olemassa olevien pro-

sessien toimivuutta kriisitilanteessa ja testataan olemassa olevien suunnitelmien toimivuus käytännössä. Harjoittelulla voidaan mitata esimerkiksi todellinen uhan toteutumisen jälkeinen häiriöaika ja toimintotason lasku. Tulosten pohjalta voidaan tehdä muutoksia edunsaajaorganisaation toimintatavoissa. Tyypillisesti harjoittelussa toimitaan yhteistoiminnassa viranomaisten tai muiden organisaatioiden kanssa. Kybertilannekeskustoimintaan kuuluu verkostoituminen ja aktiivinen osallistuminen tiedonvaihtoon. Tämä mahdollistaa viimeisimpien kyberavaruuden muutosvoimien tuntemuksen ja etukäteisen varautumisen.

2. Yhteistyössä edunsaajaorganisaation kanssa tehtävät varautumissuunnitelmat eli jatkuvuus- ja toipumissuunnitelmat toimivat prosessien kehittämisen ohjenuorina. Jatkuvuussuunnittelussa kybertilannekeskus ottaa huomioon välittömästi häiriön jälkeen tarvittavat toimet. Toipumissuunnitelmien luominen ja toteuttaminen, kuten yksityiskohtaiset toimenpiteet häiriöstä palautumiseksi kuuluvat kybertilannekeskuksen toimintaan.
3. Tilannetietoisuusprosessin jatkuva parantaminen, tilannekuvan muodostamisessa auttavien työkalujen ja automatisaation lisääminen sekä toimivat vastuunjaot tilanneymmärryksen jälkeen tehtävän tilannevasteen toteuttamiseksi ovat kybertilannekeskuksen leipätyötä.

7.2.3 Kybertilannekeskuksen vaikutus organisaation ihmisten toimintaan

Ihmiset vaikuttavat organisaation kyberresilienssiin (1) koulutuksen ja taitojen, (2) ajattelutapojen ja kyseenalaistavan asenteen perusteella sekä (3) kokemuksen ja kypsyyden tasolla (kuvio 23).

1. Kybertilannekeskuksen rungon muodostaa koulutettu ja tarvittavat tietotekniset, prosessi- sekä ryhmätyöskentelytaidot osaava henkilökunta. Henkilökunnan osaaminen on ratkaisevaa nopeista häiriötilanteista toipumiseksi ja nopeiden ratkaisujen aikaansaamiseksi.
2. Henkilökunnan huolehtiva eli asianomistajalähtöinen ajattelutapa kyberturvallisuusasioihin ja kriittinen asenne omien käytänteiden sekä toimintatapojen riittävyydestä korostuvat kybertilannekeskustoiminnassa.

3. Kybertilannekeskuksessa työskentelevien ihmisten aiempi kokemus kyberturvallisuusalalta ja operatiivisista kyberresilienssin ylläpitotehtävistä keskitetään kybertilannekeskuksissa toimivaan henkilökuntaan. Ammattitaitoisesti kypsällä ja kokeneella henkilökunnalla on suuri merkitys kyberresilienssin parantamisessa.

7.2.4 Kybertilannekeskuksen vaikutus organisaation johtamiseen

Johtaminen ja johtajat vaikuttavat organisaation kyberresilienssiin (1) asenteellaan, kiinnostuksellaan ja kyvyillään. Myös (2) resurssien käyttäminen, riittävyys ja laadukas suunnittelu vaikuttavat organisaation kyberresilienssiin. Lisäksi organisaation kyberresilienssiin vaikuttavat (3) päätösten selkeys ja nopeus (kuvio 23).

1. Kybertilannekeskuksen ja edunsaajaorganisaation johtajien asenteet kyberturvallisuusasioita kohtaan vaikuttavat organisaation kyberresilienssiin. Välinpitämättömyys, tietämättömyys ja ymmärtämättömyys vaikuttavat kyberresiliensiä alentavasti. Kybertilannekeskuksen toimialueeseen kuuluvat säännölliset raportit, tilastot ja havainnollistukset, joilla tuodaan edunsaajaorganisaation ylimmälle johdolle tietoa kyberavaruuden turvallisuustilanteen kehittymisestä. Näin kybertilannekeskus voi vaikuttaa organisaation kyberresilienssiin parantavasti.
2. Kybertilannekeskuksessa edunsaajaorganisaation myöntämien resurssien käytön suunnittelu on keskitettyä ja hallittua. Kybertilannekeskus voi tehdä tutkimustietoon pohjautuvia esityksiä lisäresurssien tarpeesta kyberresilienssin tason pitämiseksi hyväksyttävällä tasolla. Samalla voidaan ohjatusti suunnitella, millaisia erillisiä kybertilannekeskuksen ulkopuolisia erityisosaamista vaativia palveluita on tarvittaessa mahdollista hankkia. Tällainen verkostoituminen ja erityisosaamisen puutteen tunnistaminen on tärkeää poikkeamatilanteista selviytymiseksi.
3. Päätöksenteon selkeyden ja nopeuden jatkuva kehittäminen tukee häiriötilanteissa toimimista vastuukysymysten ollessa selkeitä. Nopeaa reagointia vaativissa tilanteissa tarvittavien vastuullisten henkilöiden yhteystietojen tulee olla nopeasti saatavilla, jotta toipuminen voidaan aloittaa mahdollisimman aikaisessa vaiheessa. Päätöksentekoketjujen etukäteinen määrittely vähentää väärinymmärrysten riskiä. Tällä tavoin voidaan paremmin varmistaa poikkeustilanteiden käsitteleminen järkevällä vasteaikaa lyhentävällä tavalla.

7.2.5 Kybertilannekeskuksen muut vaikutukset

Kybertilannekeskuksella voidaan teoreettisen mallin ja asiantuntijahaastatteluiden perusteella vaikuttaa edunsaajaorganisaation monilla tavoin negatiivisesti eli kyberresilienssiä huonontavalla tavalla.

Esimerkiksi ulkoistettu ja ostettu kybertilannekeskuspalvelu voi luoda illuusion hyvästä kyberresilienssistä todellisen tilanteen ollessa päinvastainen. Kybertilannekeskuksen tulee toimia edunsaajaorganisaation tarpeiden mukaisesti – ei toisin päin.

Kybertilannekeskus, jonka keinoista tulee tavoitteita ja tavoitteista keinoja on kallis, ei vastaa odotuksia, eikä paranna organisaation kyberresilienssiä optimaalisesti. Esimerkiksi vasta perustetulta kybertilannekeskusorganisaatiolta ei voida odottaa vastaavia kyberresilienssiä parantavia vaikutuksia, kuin pitkään toimineelta ja korkean kypsyystason omaavalta kybertilannekeskukselta. Kybertilannekeskuksen kypsyystason nostamiseen kuluu vuosia ja sen perustaminen ja ylläpito on kallista.

Kybertilannekeskus ei ole ratkaisu organisaation kaikkiin ongelmiin, vaan työkalu organisaation kyberresilienssin parantamiseksi.

Kybertilannekeskuksella **ei voida** suoraan vaikuttaa haitallisten tapahtumien määrään tai laatuun edunsaajaorganisaation ulkopuolisessa kyberavaruudessa. Lisäksi on huomattava, että kybertilannekeskuksella ei voida varautua kaikkiin odottamattomiin uhkiin aukottomasti. Kybertilannekeskustoiminta ei tästä johtuen takaa kyberpoikkeamien loppumista, vaan parantaa todennäköisyyttä selvitä ja lieventää niiden aiheuttama seurauksia resilientisti.

7.3 Suhde muihin tutkimuksiin

Tarkasteltaessa kriittisesti tutkimustuloksen yhtenevyyttä muiden viimeaikaisten kyberresilienssistä tehtyjen tutkimusten suhteen, voidaan todeta tutkimustuloksen olevan yhteneväinen muun resilienssitutkimuksen kanssa. Esimerkiksi järjestelmäteoreettinen holistinen organisaatioiden kokonaisvaltaisuutta ja mukautumiskykyä korostava näkökulma on laajasti hyväksytty, eikä tässä tutkimuksessa ole ilmennyt tätä käsitystä horjuttavia tosiseikkoja.

Kybertilannekeskuksen tai vastaavaa toimintaa harjoittavan organisaation vaikutuksia organisaatioiden kyberresilienssiin on tutkittu melko vähän aihealueen nopean ja viimeaikaisen kehittymisen ohella. Tämä siitä huolimatta, että kybertilannekeskuksen teknisiä toimintaedellytyksiä ja ratkaisuja ongelmiin on tutkittu viime vuosina maailmanlaajuisesti suhteellisen paljon.

Vähemmälle huomiolle on jäänyt ihmisten, prosessien ja johtamisen vaikutukset kybertilannekeskuksien toiminnassa. Aihealueesta tarvitaan lisää tieteellistä tutkimusta, jotta kybertilannekeskustoimintaa voidaan mitata kokonaisvaltaisemmin kyberresilienssin näkökulmasta.

8 JOHTOPÄÄTÖKSET

Tässä tutkimusraportin päättävässä luvussa pohditaan tutkimuksen yhteiskunnallista merkitystä, mahdollisia jatkotutkimuskohteita ja kybertilannekeskusten tulevaisuutta.

Nykyorganisaatiot eli ihmisistä koostuvat tavoitteelliset järjestelmät toimivat yhtä aikaa fyysisessä ja kybermaailmassa. Organisaatiot ovat digitalisaation myötä yhä riippuvaisempia kyberavaruuden mahdollisuuksista ja haasteista. Monille nykyorganisaatioille kyberavaruus on toiminnan elinehto. Pankit, verkkokaupat, mediatalot, teollisuus, energiantuotanto, tietotekniikkasektori, valtionhallinto ja monet muut käyttävät hyödykseen kyberavaruuden tuomia mahdollisuuksia parantaakseen toimintaedellytyksiään.

Jokaisella organisaatiolla on haaste tietää, mitä kyberavaruudessa tapahtuu ja miten varmistaa oman organisaation selviäminen muuttuvissa olosuhteissa. Monet nykyorganisaatiot ovat pimennossa kyberavaruuden tapahtumille ja luottavat tuuriin toiminnassaan. Näin toimitaan huolimatta siitä, että kyberavaruus on monelle organisaatiolle jokapäiväisen toiminnan ja selviytymisen edellytys. Organisaatiot toimivat avoimina järjestelminä jatkuvasti kyberavaruuden kanssa vuorovaikuttaen, tavoitteenaan ympäristön tarpeiden tyydyttäminen. Nykyään tämä on hyvä harvemmin mahdollista ilman kyberavaruuden tuomia hyötyjä.

Nykyorganisaatiot hyötyvät kybertilannekeskuksesta kyberavaruuden tilannetietoisuuden ja kyberresilienssin kehittymisen mahdollistajana. Kybertilannekeskuksessa – kyberavaruuden hermokeskuksessa – kyberaistien tuottamat tilannetiedot jalostuvat viisaiksi päätöksiksi. Tässä toiminnassa yhdistyvät varautuminen haasteisiin ja tarvittavat keinot poikkeamiin vastaamiseksi. Kybertilannekeskuksissa varautuminen ja tilannetietoisuus yhdistyvät ihmisten, prosessien, teknisten ratkaisuiden ja johtamisen yhdistelmänä.

Tämän tutkimusraportin merkittävin yhteiskunnallinen arvo on sovelletussa teoreettisessa mallissa, joka kuvaa kybertilannekeskuksen vaikutusta organisaation resilienssiin (kuvio 21). Lisäksi yhteiskunnallisesti arvokkaana voidaan pitää aineistoanalyysin ja aikaisemman tutkimuskirjallisuuden pohjalta löydettyjä organisaation kyberresilienssiin vaikuttavia tekijöitä (kuvio 23). Tämän tutkimuksen tietojen avulla kybertilannekeskuspalveluntarjoajat

(MSSP) tai organisaatioiden omat kybertilannekeskukset voivat yhteistyössä edunsaajaorganisaation kanssa hahmottaa jäsennellymmin organisaation kyberresilienssiin vaikuttavia tekijöitä.

Tämän tutkimuksen tutkimuksellinen arvo on erityisesti hallintotieteellinen ja organisationaalinen – prosesseja, johtamista ja ihmisiä koskettava. Teknisiä järjestelmiä käsiteltiin tässä tutkimusraportissa vain tarpeellisin osin, eikä tutkimuksen tarkoituksena ollut tutkia jo hyvin laajasti kirjallisuudessa käsiteltyä kybertilannekeskusten teknistä toimintaa.

Mahdollisia jatkotutkimuskohteita ovat esimerkiksi kybertilannekeskuksen kyberresilienssivaikutusten tarkempi kvalitatiivisten ja kvantitatiivisten mittareiden kehittäminen. Tarkemmilla mittareilla voitaisiin tarkasti mitata kybertilannekeskusten vaikutuksia organisaation kyberresilienssiin. Tämän lisäksi olisi hyödyllistä tutkia kybertilannekeskusten yleisyyttä, käyttötapauksia ja jo kybertilannekeskuksen perustaneiden yritysten motiiveja perustamisen taustalla.

Mielenkiintoista olisi lisäksi tietää, miten kybertilannekeskuspalvelua myyvien yritysten (MSSP) ja edunsaajaorganisaation osana olevan kybertilannekeskuksen vaikutukset kyberresilienssiin eroavat toisistaan. Kybertilannekeskushan toimii monissa asioissa hyvin tiiviissä yhteistyössä edunsaajaorganisaation kanssa. Tästä syystä olisi mielenkiintoista tietää, millainen vaikutusero kyberresilienssiin on ostetun ulkoistetun palvelun ja oman organisaation tuottaman palvelun välillä.

Tutkimusprosessissa onnistuminen voidaan kiteyttää siihen, kuinka hyvin tutkimus vastaa tutkittavaan asiaan eli tutkimuskysymykseen. Tämän tutkimuksen tarkoituksena on ollut vastata kysymykseen: Miten kybertilannekeskus vaikuttaa organisaation kyberresilienssiin? Tutkimuskysymykseen on vastattu täsmällisesti, seikkaperäisesti ja samalla monipuolisesti – holistisesti.

Tutkimusraportin ulkonäköön, kuvioihin ja selvennyksiin on kiinnitetty erityistä huomiota abstraktin ja vaikeasti muutoin lähestyttävän aiheen takia. Tutkimusprosessin aikana on jatkuvasti pyritty punnitsemaan, tukeeko kirjoitettu teksti tutkimuskysymykseen vastaamista. Ylimääräiset ja tarpeettomat osat on karsittu pois monien iteraatiokierrosten avulla.

Tutkimuksen lähdekritiikki on ollut tarkkaa. Monissa tapauksissa on käytetty alkuperäislähteitä ja vain harvoin on jouduttu tukeutumaan sekundäärilähteisiin. Tutkimuksessa on

käytetty yli kahtasataa erilaista tieteellistä ja muuta lähdettä, joiden avulla on lisätty tutkimuksen validiteettia ja reliabiliteettia, joissa on onnistuttu melko hyvin.

Tutkimuksen tekemisessä tarvittavaa kriittistä otetta on pidetty tärkeänä erityisesti liian pitkälle menevien kausaalipäätelmien välttämiseksi ja syy-seuraussuhteiden selvittämiseksi. Interpretivististä eli tulkinnallisuutta korostavaa tutkimusstrategiaa noudattaen on korostettu tutkijan tulkinnan ja hermeneuttisen kehän avulla jalostuvaa käsitystä kybertilannekeskusten vaikutuksesta organisaatioiden kyberresilienssiin.

Teemahaastattelut onnistuivat hyvin ja kaikki haastateltavat kehuivat haastattelutilannetta opettavaiseksi. Samalla kerätty laaja aineisto tarjosi mahdollisuuden pitkälle menevään analyysin, jonka tulokset on esitetty tässä tutkimusraportissa. Teemahaastatteluiden valinta tiedonkeruumenetelmäksi tuki hyvin interpretivististä tutkimusstrategiaa ja tarjosi mahdollisuuden uuden tiedon tuottamiseksi vähän tutkitusta aihealueesta.

Tutkimuksen rungon muodostaa laaja systeemiteoriaan pohjautuva teoreettisten mallien katsaus ja niiden sovellettu yhdistäminen, joka asetti tutkimukselle suurimmat haasteet. Kriittisen pohdinnan, kirjallisuuden ja aineiston avulla muodostettu teoreettinen malli on kuitenkin yksi tutkimuksen suurimmista saavutuksista, sillä tiedossa ei ole, että kukaan olisi aikaisemmin kuvannut kybertilannekeskuksen toimintaa vastaavalla tavalla olemassa olevia teoreettisia malleja soveltaen.

Kybertilannekeskusten tulevaisuus näyttää valoisalta. Keskuksia perustetaan jatkuvasti lisää ja tarve kasvaa jatkuvasti. Tämä tutkimus voi osaltaan olla vaikuttamassa organisaatioiden kyberturvallisempaan huomiseen tutkitun uuden tiedon avulla ja samalla parantaa yhteiskunnan kyberturvallisuuden tasoa omalta pieneltä osaltaan.

LÄHTEET

Acharya Rajendra, Ng Eddie & Suri Jasjit. (2008). Image modeling of the human eye. USA: Artech House.

Adriaans Pieter. (2010). A Critical Analysis of Floridi's Theory of Semantic Information. Knowledge, Technology & Policy 23(1-2): 41-56.

Ahsan Syed & Shah Abad. (2006). Data, Information, Knowledge, Wisdom: A Doubly Linked Chain. 2006 International Conference on Information and Knowledge Engineering. Las Vegas, Nevada, USA: Citeseer: 270-278.

Ampère André-Marie. (1834). Essai sur la philosophie des sciences. Paris: Bachelier.

Apostolopoulos Nikolaos, Newbery Robert & Gkartzios Menelaos. (2018). Social enterprise and community resilience: Examining a Greek response to turbulent times. Journal of Rural Studies.

Aristoteles. (noin 300 e.a.a.). Metaphysics. Haettu osoitteesta: http://data.perseus.org/citations/urn:cts:greekLit:tlg0086.tlg025.perseus-eng1:8.1045a.(3.6.2019).

Barley Stephen & Kunda Gideon. (1992). Design and Devotion: Surges of Rational and Normative Ideologies of Control in Managerial Discourse. Administrative Science Quarterly 37(3): 363-399.

Bartuskova Aneta & Krejcar Ondrej. (2014). The Evolutionary Approach of General Systems Theory Applied to World Wide Web. Second International Conference, ICCASA 2013. Vietnam: Springer International Publishing: 188-197.

Benington John & Moore Mark. (2011). Public value: Theory and practice. New York: Palgrave Macmillan.

Berger Christoph, Hees Andreas, Braunreuther Stefan & Reinhart Gunther. (2016). Characterization of cyber-physical sensor systems. Procedia CIRP 41: 638-643. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S2212827115010987.

Berlin Amanda & Brotherston Lee. (2017). Defensive security handbook. USA: O'Reilly Media, Inc.

Beynon-Davies Paul. (2011). Significance: Exploring the nature of information, systems and technology. England, Hampshire: Palgrave Macmillan.

Blom Raimo, Melin Harri & Pyöriä Pasi. (2001). Tietotyö ja työelämän muutos: Palkkatyön arki tietoyhteiskunnassa. Helsinki: Gaudeamus.

Boddy Sara & Shattuck Justin. (2018). Cyber attacks spike in Finland before Trump-Putin meeting. Haettu osoitteesta: https://www.f5.com/labs/articles/threat-intelligence/cyber-attacks-spike-in-finland-before-trump-putin-meeting.(30.5.2019).

Boulding Kenneth. (1956). General Systems Theory - The Skeleton of Science. Management Science 2(3): 197-208.

Brown Judith, Greenspan Steven & Biddle Robert. (2016). Incident response teams in IT operations centers: The T-TOCs model of team functionality. Cognition, Technology & Work 18(4): 695-716.

Bublitz Wolfram & Hoffmann Christian. (2017). Pragmatics of social media. Berlin; Boston: De Gruyter.

Burnard Kevin & Bhamra Ran. (2011). Organisational resilience: development of a conceptual framework for organisational responses. International Journal of Production Research 49(18): 5581-5599.

Cáceres Mario, Lachuer Joel, Zapala Matthew, Redmond John, Kudo Lili, Geschwind Daniel, Lockhart David, Preuss Todd & Barlow Carrolee. (2003). Elevated Gene Expression Levels Distinguish Human from Non-Human Primate Brains. Proceedings of the National Academy of Sciences of the United States of America 100(22): 13030-13035.

Chamiekara G., Cooray M., Wickramasinghe L., Koshila Y., Abeywardhana Kavinga & Senarathna Amila. (2018). AutoSOC: A Low Budget Flexible Security Operations Platform for

Enterprises and Organizations. 2017 National Information Technology Conference (NITC). Sri Lanka: IEEE 1: 100-105.
Chamovitz Daniel. (2012). What a plant knows: A field guide to the senses. USA: Scientific American / Farrar, Straus and Giroux.
Chan Gary & Jin Xing. (2010). Unstructured Peer-to-Peer Network Architectures. Kirjassa: Xuemin Sherman, Yu Heather, Buford John & Akon Mursalin (eds) Handbook of Peer-to-Peer Networking. Boston, MA: Springer US: 117-142.
Chandler Daniel & Munday Rod. (2016). Deep web. A Dictionary of Media and Communication. Haettu osoitteesta: http://tuni.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwtV2xTsNADLVQB2CiCBDQgvoBpCTnJnFGQAQWJmAXRJHYklQ1f4C3419USICUwemDHeycsnJfnf2ewZAswyDXz6BsoJMIcGRaheXWEdO4kpJpMTHKkyUN_z-Qve5HPhJzo193l2LLFtPnBs33dBb814L6dYJvKpVKVbQSkQqkOnzC6pMGHWDwWgwYHE8SJ56nWoV2NPda78FDQocSpMhwgtASATRxx397UfkyY_gq-fvDM0UNtvmYylb4o-g43-uYwoHgybtMexxcwL7FfPnQtzwKWD--PbwHMjL23bd2i7ljNabsyNzVsCgVYN4BpOmbfgcFhRzZMoMHWGxyrTPlXOpTg-JK1fxBdzsYvlyt-kzOBR4kmjFl1nNYbJZb_lKHvKVr_1f-wZTdqPj.
Chen Thomas & Abu-Nimeh Saeed. (2011). Lessons from Stuxnet. Computer 44(4): 91-93.
Christian Michael, Sprung Charles, King Mary, Dichter Jeffrey, Kissoon Niranjan, Devereaux Asha & Gomersall Charles. (2014). Triage: Care of the critically ill and injured during pandemics and disasters: CHEST consensus statement. Chest 146(4): e61-e74S. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S0012369215519909.
Clarke Richard & Knake Robert. (2010). Cyber war: The next threat to national security and what to do about it. New York: Harper Collins.
Clegg Stewart & Hardy Cynthia. (1999). Studying organization. GB: Sage Publications Ltd.
Coe Taylor. (2015). Where is the origin of 'cyber'?. Haettu osoitteesta: https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/.(16.5.2019).
Cooper Paul. (2017). Data, information, knowledge and wisdom. Anaesthesia & Intensive Care Medicine 18(1): 55-56. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S1472029916301813.
CSIS. (2019). Significant cyber incidents since 2006. Center for Strategic and International Studies: 1-37. Haettu osoitteesta: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity. (26.4.2019).
Daigle Leslie. (2004). WHOIS protocol specification. Draft Standard. Haettu osoitteesta: https://tools.ietf.org/html/rfc3912.
Dalziel Henry. (2014). How to define and build an effective cyber threat intelligence capability. Waltham, Massachusetts: Syngress.
Das Krishna & Spicer Jonathan. (2016). How the New York fed fumbled over the Bangladesh bank cyber-heist. Haettu osoitteesta: https://www.reuters.com/investigates/special-report/cyber-heist-federal/.(30.5.2019).
Dasgupta Ranjan, Chattopadhyay Dhiman, Pal Arpan & Chakravarty T. (2014). A Comprehensive Seven Layer Sensor Model: Cyber-Physical System. Kirjassa: Mason Alex, Mukhopadhyay Subhas Chandra, Jayasundera Krishanthi & Bhattacharyya Nabarun (eds) Sensing Technology: Current Status and Future Trends. Cham: Springer International Publishing: 57-81.
Demertzis Konstantinos, Kikiras Panayiotis, Tziritas Nikos, Sanchez Salvador & Iliadis Lazaros. (2018). The Next Generation Cognitive Security Operations Center: Network Flow Forensics Using Cybersecurity Intelligence. Big Data and Cognitive Computing 2(4): 35.
Dufva Mikko, Laine Paula, Vataja Katri, Lähdemäki-Pekkinen Jenna & Parkkonen Pinja. (2019). Tulevaisuusbarometri 2019. Sitran selvityksiä: 39.
Dusia Ayush & Sethi Adarshpal. (2018). Probe generation for active probing. International Journal of Network Management 28(4): e20.
Dyson George. (1997). Darwin among the machines. USA: Addison-Wesley.

Encyclopædia Britannica. (2018a). Domain Name System (DNS). Haettu osoitteesta: http://tuni.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwY2AwNtIz0EUrE0wsLZKNDNKSU03M04xNEy2SDUxNU5KBrbs0ixRzgyRQxIf6Wji5ATv8Ft6IkYxE6BpxvdQkyAQqaCFNsX4yuE8NdHqqPjR89U1AJ6eDekHAJjAofzp5h3AzcCWBOth5oF0WSJWGmwBDFGzrDfwehJLSvEw9YGxinMVIqhMEGTjhR8QKMTCl5okAG2p-waIM0m6uIc4euggnxacmxUP0GIsxsAA7-6kSDAqJRikWhmnmqeaGponA7JUEbH8ZJZsYWiYZmAEDzTBVkkEEmwlS2IWlGbiAFbwFaCzS0ECGgaWkqDRVFkgBPSsHDiMg6e0TAQBrCHrH.(17.8.2019).

Encyclopædia Britannica. (2018b). Search engine. Haettu osoitteesta: http://tuni.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwlV1LCwIhEB6iS9uloqI3_YH24W5k16Il2LoVRJdFZYIue6jt_zdjT6pLIAqCMo7j41PnEyAUrj_6mBPMdCwilCj4N3gjpBKCDCdA7WsKEbsSb9dyFhPgl8nrJEPd34i7qG8XqPyQ5uwZi6lJdPTuvVCZpnkqZi2wDw-Z8mmDI5mgJ2xl8XbohFXYP9wvXn-g5BfsqNLvfnFxfiv-CFUoPSlia1DArE7WbY12iJZhsAH-deLGZL0cv4VLU6a102IQiwX5swVBbrjhf0QJyiCah0oSBJ0YpDFAaVEEb6r9q6PzO7oJ-Dupd8Khn4PSjmpwv2KaFmD6y2KE5WuyspIX-5.(17.8.2019).

Endsley Mica. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors: The Journal of the Human Factors and Ergonomics Society 37(1): 32-64.

English Oxford Living Dictionaries. (2019a). Observation. Haettu osoitteesta: https://en.oxforddictionaries.com/definition/observation.(7.6.2019).

English Oxford Living Dictionaries. (2019b). Perception. Haettu osoitteesta: https://en.oxforddictionaries.com/definition/perception.(7.6.2019).

ETN. (2018). Neuromorfinen tietokone ratkaisee datavyöryn ongelman. Haettu osoitteesta: http://etn.fi/index.php/13-news/7373-neuromorfinen-tietokone-ratkaisee-datavyoryn-ongelman.(10.6.2019).

Etzioni Amitai. (1970). Nykyajan organisaatiot. Helsinki: Tammi.

Falliere Nicolas, Murchu Liam & Chien Eric. (2011). W32. Stuxnet dossier. White paper, Symantec Corporation, Security Response 5(6): 29.

Fan Wenjun, Du Zhihui, Fernandez David & Villagra Victor. (2017). Enabling an Anatomic View to Investigate Honeypot Systems: A Survey. IEEE Systems Journal 12(4): 3906-3919.

Finkle Jim. (2011). Exclusive: Nasdaq hackers spied on company boards. Haettu osoitteesta: https://www.reuters.com/article/us-nasdaq-hacking/exclusive-nasdaq-hackers-spied-on-company-boards-idUSTRE79J84T20111020.(30.5.2019).

Foucault Michel. (1995). Discipline and punish: The birth of the prison. New York: Vintage.

Fuegi John & Francis Jo. (2003). Lovelace & Babbage and the creation of the 1843 'notes'. IEEE Annals of the History of Computing 25(4): 16-26.

Gadamer Hans-Georg & Linge David. (1977). Philosophical hermeneutics. Berkeley / Los Angeles, California, USA: University of California Press.

Gallistel Charles. (1989). Animal Cognition: The Representation of Space, Time and Number. Annual Review of Psychology 40(1): 155-189.

Garofalo Charles. (2015). Where Should We Draw the Line?: Governance, Public Values, and Outsourcing National Security. Public Integrity 17(2): 189-202.

Gibson William. (1986a). Burning chrome. New York, USA: Arbor House.

Gibson William. (1986b). Neuromancer. Pennsylvania State University: Phantasia Press.

Glosbe. (2019a). Cybernetics. Haettu osoitteesta: https://glosbe.com/en/grc/cybernetics.(5.4.2019).

Glosbe. (2019b). Κυβερνάω. Haettu osoitteesta: https://glosbe.com/grc/en/%CE%BA%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%AC%CF%89.(5.4.2019).

Goldman Sachs. (2017). Is 'FANG' mispriced? Haettu osoitteesta: https://www.academia.edu/34119440/Is_FANG_mispriced.(15.6.2019).

Google LLC. (2019). Tietojen järjestäminen indeksoimalla. Haettu osoitteesta: https://www.google.com/intl/fi/search/howsearchworks/crawling-indexing/.(27.5.2019).

Groot Sybren Ruurds de & Mazur Peter. (1984). Non-equilibrium thermodynamics. New York: Dover Publications Inc.
Guillén Mauro. (1994). Models of management: Work, authority, and organization in a comparative perspective. Chicago and London: The University of Chicago Press.
Haapala Timo. (2013). MTV3: Suomen ulkoministeriö laajan verkkovakoilun kohteena vuosia. Haettu osoitteesta: https://www.mtvuutiset.fi/artikkeli/mtv3-suomen-ulkoministerio-laajan-verkkovakoilun-kohteena-vuosia/2369718#gs.f34any.(30.5.2019).
Haikonen Pentti. (2017). Tietoisuus, tekoäly ja robotit. Helsinki: Art House Oy.
Halfpenny Peter. (1979). The Analysis of Qualitative Data. The Sociological review 27(4): 799-827.
Hallamaa Teemu. (2014). Kohuelokuva The Interview julkaistaan netissä jo tänään. Haettu osoitteesta: https://yle.fi/uutiset/3-7707480.(5.6.2019).
Hámornik Balázs Péter & Krasznay Csaba. (2018). A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers. International Conference on Applied Human Factors and Ergonomics. Cham: Springer International Publishing: 224-236.
Haraty Ramzi & Zantout Bassam. (2014). The TOR data communication system. Journal of Communications and Networks 16(4): 415-420.
Harisalo Risto. (2008). Organisaatioteoriat. Tampere: Tampere University Press.
Harper Douglas. (2019). System (noun). Haettu osoitteesta: https://www.etymonline.com/word/system.(21.4.2019).
Herzog Stephen. (2011). Revisiting the Estonian Cyber Attacks; Digital Threats and Multinational Responses. Journal of Strategic Security 4(2): 49-60.
Hirsjärvi Sirkka, Remes Pirkko & Sajavaara Paula. (1997). Tutki ja kirjoita. Tampere: Kirjayhtymä Oy.
Hodges Andrew. (2012). Alan Turing. London: Random House.
Holling Crawford. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics 4(1): 1-23.
Hyman Anthony. (1982). Charles Babbage - pioneer of the computer. USA: Princeton University
Hyvönen Ari-Elmeri, Juntunen Tapio, Mikkola Harri, Käpylä Juha, Gustafsberg Harri, Nyman Markku, Rättilä Tiina, Virta Sirpa & Liljeroos Johanna. (2019). Kokonaisresilienssi ja turvallisuus: Tasot, prosessit ja arviointi. Helsinki: Valtioneuvoston kanslia.
ICANN. (2015). Threats, vulnerabilities and exploits – oh my! Haettu osoitteesta: https://www.icann.org/news/blog/threats-vulnerabilities-and-exploits-oh-my.(25.5.2019).
Ihanus Juhani & Pakarinen Hilkka. (2010). Ekvifinaliteetti. Haettu osoitteesta: https://www.avoin.helsinki.fi/oppimateriaalit/psykologia/avoin-sanasto.htm.(29.5.2019).
Indiveri Giacomo, Linares-Barranco Bernab, Hamilton Tara, van Schaik André, Etienne-Cummings Ralph, Delbruck Tobi, Liu Shih-Chii, Dudek Piotr, Häfliger Philipp, Renaud Sylvie, Schemmel Johannes, Cauwenberghs Gert, Arthur John, Hynna Kai, Folowosele Fopefolu, Saighi Sylvain, Serrano-Gotarredona Teresa, Wijekoon Jayawan, Wang Yingxue & Boahen Kwabena. (2011). Neuromorphic Silicon Neuron Circuits. Frontiers in Neuroscience 5(73): 1-23.
International Organization for Standardization. (2011). ISO/IEC 27031:2011 information technology — security techniques — guidelines for information and communication technology readiness for business continuity. ISO/IEC 27031:2011(en) Haettu osoitteesta: https://www.iso.org/obp/ui/#iso:std:iso-iec:27031:ed-1:v1:en.
International Organization for Standardization. (2012). ISO/IEC 27032:2012: Information technology. security techniques. guidelines for cybersecurity. Haettu osoitteesta: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.(24.4.2019).
International Organization for Standardization. (2018). ISO/IEC 27000:2018(en). Haettu osoitteesta: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.(24.4.2019).
International Electrotechnical Commission. (1993). Johtokoodi. Haettu osoitteesta: http://www.tsk.fi/tepa/fi/haku/johtokoodi.(28.4.2019).

Jennett Bryan & Plum Fred. (1972). Persistent vegetative state after brain damage: A Syndrome in Search of a Name. The Lancet 299(7753): 734-737.
Jetty Sairam. (2018). Network scanning cookbook. GB: Packt Publishing.
Joint Chiefs of Staff. (2013). JP 2-0, joint intelligence. Joint Electronic Library: Joint Chiefs of Staff.
Keeley Brian. (2015). Nonhuman Animal Senses. Kirjassa: Mohan Matthen (ed) The Oxford Handbook of Philosophy of Perception. USA: Oxford University Press.
Kerkkänen Tuomas. (2016). Viaton klikkaus sähköpostissa – näin venäjän verkkovakoojat iskivät ulkoministeriöön. Haettu osoitteesta: https://yle.fi/uutiset/3-8591029.(30.4.2019).
Kerkkänen Tuomas & Pietarinen Eetu. (2016). Venäläisen verkkovakoojan 12 askelta suomen ulkoministeriön koneille ja jälkien peittämiseen. Haettu osoitteesta: https://yle.fi/uutiset/3-8591034.(30.4.2019).
Kivimäki Veli-Pekka. (2017). Avointen lähteiden tiedustelu (OSINT). Informaation hallinta ja tiedustelu 1.
Kokar Mieczyslaw & Endsley Mica. (2012). Situation Awareness and Cognitive Modeling. IEEE Intelligent Systems 27(3): 91-96.
Konttinen Matti. (2019). KRP tutkii vaalien tulospalveluun kohdistettua palvelunestohyökkäystä – vaalijohtaja: "Lyhyt ja heikko". Haettu osoitteesta: https://yle.fi/uutiset/3-10731312.(30.4.2019).
Kotimaisten kielten keskus. (2019). Reaktioita: Vaikutus ja merkitys. Haettu osoitteesta: http://www.kielitoimistonohjepankki.fi/haku/merkitys/ohje/619.(12.5.2019).
Kraut Richard. (2004). Stanford encyclopedia of philosophy. Haettu osoitteesta: https://plato.stanford.edu/entries/plato/.(5.4.2019).
Kyberturvallisuuskeskus. (2019). Yhteistyöverkostot. Haettu osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen.(26.5.2019).
Laboratory BioMag. (2016). The structure and operation of the human brain - Näköaisti. Haettu osoitteesta: https://www.biomag.hus.fi/braincourse/L5.html.(5.6.2019).
Lähdesmäki Tuuli, Hurme Pertti, Koskimaa Raine, Mikkola Leena & Himberg Tommi. (2015). Menetelmäpolkuja humanisteille. Haettu osoitteesta: http://www.jyu.fi/mehu.(13.5.2019).
Laine Petrus. (2017). Intel esitteli neuromorfisen Loihi-prosessorin. Haettu osoitteesta: https://www.io-tech.fi/uutinen/intel-esitteli-neuromorfisen-loihi-prosessorin/.(22.5.2019).
Laureys Steven, Owen Adrian & Schiff Nicholas. (2004). Brain function in coma, vegetative state, and related disorders. Lancet Neurology 3(9): 537-546.
Lee Robert, Assante Michael & Conway Tim. (2014). German steel mill cyber attack. Industrial Control Systems: 1-15. Haettu osoitteesta: https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.
Lehto Martti, Limnéll Jarno, Kokkomäki Tuomas, Pöyhönen Jouni & Salminen Mirva. (2018). Kyberturvallisuuden strateginen johtaminen suomessa. Valtioneuvoston kanslia: 1-105. Haettu osoitteesta: https://tietokayttoon.fi/documents/10616/6354562/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf/efea3c33-3c74-4cf6-b237-d49b4f10ab83/28-2018-Kyberturvallisuuden+strateginen+johtaminen..pdf.pdf?version=1.0.
Lemak David. (2004). Leading students through the management theory jungle by following the path of the seminal theorists. Management Decision 42(10): 1309-1325.
Linkov Igor, Eisenberg Daniel, Plourde Kenton, Seager Thomas, Allen Julia & Kott Alex. (2013). Resilience metrics for cyber systems. Environment Systems and Decisions 33(4): 471-476.
Lodish Harvey, Berk Arnold, Kaiser Chris & Krieger Monty. (2000). Overview of Neuron Structure and Function. Kirjassa: Lodish Harvey, Berk Arnold & Kaiser Chris (eds) Molecular Cell Biology. New York: W.H. Freeman Macmillan Learning.
Logsdon Tom. (2018). GPS - global positioning system. Haettu osoitteesta: http://tuni.summon.serialssolutions.com/2.0.0/link/0/eLvHCXMwlV1LS8QwEB50L64XlVV84x9om2ebXFdchSoI9iBelmaSgJcKuvv_nXTrrqgXLwkkOQzfJPPKZAIgRc6yHzKBllpnSye1krLlGH3Fo-

jGO9pcTHPt6pg9mOiOH39SbSEY75Ijnwa0uUFMizUeBvU9NpIdiwLeQNmluEsVkAqf-zOa2bXRi75GB36ZXFN6Ux24OXr6c3638QFsvuNSdu_qrF-F8S9mFnXSL2AL-ZCN4Ht28enQ2hmN831XTZ8cZA5xUWmYgi8RIW2rCSPVlTOyIhMRC5DxSzSlJfakRZmqLT-wWBFq2uvY0pBt5RGMurcuHMMVEit0KIOK2ivvFdHNYxTKobW-leYEJhs05sHNV-Se_j18BmOyDEwKYnJ2DqPF-zJcUEcoXfbgUlvfP38CAF-K6A.(4.5.2019).

Low Philiph. (2012). The Cambridge declaration on consciousness. Haettu osoitteesta: http://fcmconference.org/img/CambridgeDeclarationOnConsciousness.pdf.(7.6.2019).

Luciano Floridi & Zalta Edward. (2019). Semantic conceptions of information. Haettu osoitteesta: https://plato.stanford.edu/archives/sum2019/entries/information-semantic/.(4.5.2019).

Lyytikkä Jyrki & Hallamaa Teemu. (2018). Kiina rakentaa verkkoa maailmalle – Googlen ex-toimitusjohtaja ennustaa, että kiinan vaikutusvallan kasvu jakaa internetin kahtia. Haettu osoitteesta: https://yle.fi/uutiset/3-10442069.(14.5.2019).

Madani Afsaneh, Rezayi Saed & Gharaee Hossein. (2011). Log Management Comprehensive Architecture in Security Operation Center (SOC). 2011 International Conference on Computational Aspects of Social Networks (CASoN). Spain: IEEE: 284-289.

Malone Rick. (2015). Protective intelligence: Applying the intelligence cycle model to threat assessment. Journal of Threat Assessment and Management 2(1): 53-62.

Manchester Triage Group. (2015). Emergency triage: Telephone triage and advice. New York: John Wiley & Sons, Incorporated.

Manzanares-Lopez Pilar, Muñoz-Gea Juan Pedro, Malgosa-Sanahuja Josemaria & Sanchez-Aarnoutse Juan. (2010). Anonymity in P2P Systems. Kirjassa: Shen Xuemin, You Heather, Buford John & Akon Mursalin (eds) Handbook of Peer-to-Peer Networking. USA: Springer US: 785-812.

Margulies Jonathan. (2015). A Developer's Guide to Audit Logging. IEEE Security & Privacy 13(3): 84-86.

Markoff John. (2013). Brainlike computers, learning from experience. Haettu osoitteesta: https://www.nytimes.com/2013/12/29/science/brainlike-computers-learning-from-experience.html?pagewanted=all&_r=0.(15.5.2019).

Mead Carver & Conway Lynn. (1980). Introduction to VLSI systems. USA: Addison-Wesley Reading.

Merriam-Webster. (2019a). Cyber. Haettu osoitteesta: https://www.merriam-webster.com/dictionary/cyber.(17.5.2019).

Merriam-Webster. (2019b). System (noun). Haettu osoitteesta: https://www.merriam-webster.com/dictionary/system.(21.5.2019).

Merriam-Webster. (2019c). Time. Haettu osoitteesta: https://www.merriam-webster.com/dictionary/time.(24.5.2019).

Merriam-Webster. (2019d). War room (noun). Haettu osoitteesta: https://www.merriam-webster.com/dictionary/war%20room.(21.5.2019).

Miller John & Page Scott. (2009). Complex adaptive systems: An introduction to computational models of social life. USA: Princeton University Press.

Mingers John. (1997). Systems typologies in the light of autopoiesis: a reconceptualization of Boulding's hierarchy, and a typology of self-referential systems. Systems Research and Behavioral Science 14(5): 303-313.

Montévil Maël & Mossio Matteo. (2015). Biological organisation as closure of constraints. Journal of theoretical biology 372: 179-191. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S0022519315001009.

MOT sanakirjat. (2019a). Resilience. Haettu osoitteesta: https://mot-kielikone-fi.libproxy.tuni.fi/mot/uta/netmot.exe.(13.5.2019).

MOT sanakirjat. (2019b). Vaikuttaa. Haettu osoitteesta: https://mot-kielikone-fi.libproxy.tuni.fi/mot/.(15.5.2019).

Muñoz Edrisi, Capón Elisabet, Laínez Jose M., Moreno-Benito Marta, Espuña Antonio & Puigjaner Luis. (2012). Operational, tactical and strategical integration for enterprise decision-

making. Computer Aided Chemical Engineering 30: 397-401. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/B9780444595195500800.
Mustajoki Pertti. (2018). Autoimmuunisairaudet. Haettu osoitteesta: https://www.terveyskirjasto.fi/terveyskirjasto/tk.koti?p_artikkeli=dlk00010.(29.5.2019).
Nadel Barbara. (2004). Building security: Handbook for architectural planning and design. USA: McGraw-Hill Education.
Nails Debra. (2005). Stanford encyclopedia of philosophy. Haettu osoitteesta: https://plato.stanford.edu/entries/socrates/.(5.4.2019).
Nair Unnikrishnan. (2001). Adaptation to creation: progress of organizational learning and increasing complexity of learning systems. Systems Research and Behavioral Science 18(6): 505-521.
Natu Maitreya & Sethi Adarshpal. (2006). Active Probing Approach for Fault Localization in Computer Networks. 2006 4th IEEE/IFIP Workshop on End-to-End Monitoring Techniques and Services. Canada: IEEE 2006: 25-33.
Niiniluoto Ilkka. (1990). Maailma, minä ja kulttuuri: Emergentin materialismin näkökulma. Helsinki: Otava.
Niiniluoto Ilkka. (1997). Johdatus tieteenfilosofiaan: Käsitteen- ja teorianmuodostus. Helsingissä: Otava.
Niiniluoto Ilkka. (2001). Tieteiden ykseys. Tieteessä tapahtuu 19(4).
Niiniluoto Ilkka & Hallinnon kehittämiskeskus. (1996). Informaatio, tieto ja yhteiskunta: Filosofinen käsiteanalyysi. Helsinki: Edita.
Norri-Sederholm Teija. (2015). Tilanne päällä. Tiedon tarpeesta jaettuun tietoon - Hätäkeskuspäivystäjän ja ensihoidon kenttäjohtajan tilannetietoisuus. Kuopio: Itä-Suomen yliopisto: 142. Haettu osoitteesta: http://urn.fi/URN:ISBN:978-952-61-1694-5 http://urn.fi/URN:ISBN:978-952-61-1694-5.
O'Kelly Morton. (2015). Network Hub Structure and Resilience. Networks and Spatial Economics 15(2): 235-251.
OECD. (2019). Measuring the digital transformation: A roadmap for the future. OECD: 1-262. Haettu osoitteesta: https://doi.org/10.1787/9789264311992-en.
Onwubiko Cyril. (2015). Cyber Security Operations Centre: Security Monitoring for Protecting Business and Supporting Cyber Defense Strategy. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). UK: Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC.ORG): 1-10.
Onwubiko Cyril. (2018). CoCoa: An Ontology for Cybersecurity Operations Centre Analysis Process. 2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). UK: IEEE: 1-8.
Oppiminen Yle. (2015). Aistit. Haettu osoitteesta: https://yle.fi/aihe/artikkeli/2015/12/15/aistit.(26.5.2019).
Ottis Rain & Lorents Peeter. (Apr 1, 2010). Cyberspace: Definition and Implications. 5th International Conference on Information Warfare and Security. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence: 267-270.
Owen Adrian, Coleman Martin, Boly Melanie, Davis Matthew, Laureys Steven & Pickard John. (2006). Detecting Awareness in the Vegetative State. Science 313(5792): 1402.
Oxford University Press. (2019). Cyber. Haettu osoitteesta: https://en.oxforddictionaries.com/definition/cyber.(17.5.2019).
Palmer Danny. (2019). Ransomware: The key lesson Maersk learned from battling the NotPetya attack. Haettu osoitteesta: https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/.(30.5.2019).
Pettit Timothy, Fiksel Joseph & Croxton Keely. (2010). Ensuring Supply Chain Resilience: Development of a conceptual framework. Journal of Business Logistics 31(1): 1-21.
Phelan Steven. (1999). A Note on the Correspondence Between Complexity and Systems Theory. Systemic Practice and Action Research 12(3): 237-246.
Pindarus & Sandys John. (1915). The odes of Pindar. London University: Heinemann University

Pirkkalainen Sanna. (2012). Juoruileva delfiini haastaa ihmisen ylivertaisen älyn. Haettu osoitteesta: https://yle.fi/uutiset/3-5531277.(25.5.2019).
Plato, Steadman Geoffrey & Burnet John. (2012). Plato's republic I. USA
Read Allen. (1999). The new international Webster's comprehensive dictionary of the English language. Chicago, Illinois: Trident Press International.
Richelle Marc & Lejeune Helga. (1980). Time in animal behaviour. Oxford University: Pergamon Press.
Ross Howard. (2014). Everyday bias: Identifying and navigating unconscious judgments in our daily lives. Blue Ridge Summit: Rowman & Littlefield Publishers.
Rouse Margaret. (2018). Explore the features of unified endpoint management. Haettu osoitteesta: https://searchmobilecomputing.techtarget.com/essentialguide/Explore-the-features-of-unified-endpoint-management.(26.5.2019).
Saaranen-Kauppinen Anita & Puusniekka Anna. (2006). KvaliMOTV - kvalitatiivisten tutkimusmenetelmien oppimisympäristö. Haettu osoitteesta: https://www.fsd.uta.fi/menetelmaopetus/kvali/L2_3_1.html.(12.3.2019).
Sahebjamnia Navid, Torabi Ali & Mansouri Afshin. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. European Journal of Operational Research 242(1): 261-273. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S0377221714007942.
Sanastokeskus TSK. (2018). Kyberturvallisuuden sanasto (TSK 52). Helsinki: Sanastokeskus TSK ry.
Santos Omar, Muniz Joseph & De Crescenzo Stefano. (2017). CCNA cyber ops SECOPS 210-255 official cert guide. USA: Cisco Press.
Scott Richard & Davis Gerald. (2015). Organizations and organizing: Rational, natural, and open systems perspectives. Upper Saddle River (N.J.): Pearson Education.
Seeck Hannele. (2008). Johtamisopit suomessa. taylorismista innovaatioteorioihin. Tallinna: Gaudeamus.
Seville Erica, Brunsdon David, Vargo John & McManus Sonia. (2008). Facilitated Process for Improving Organizational Resilience. Natural Hazards Review 9(2): 81-90.
Shah Ankit, Ganesan Rajesh, Jajodia Sushil & Cam Hasan. (2018). Optimal Assignment of Sensors to Analysts in a Cybersecurity Operations Center. IEEE Systems Journal 13(1): 1060-1071.
Shank John. (2019). André-Marie Ampère. Haettu osoitteesta: https://www.britannica.com/biography/Andre-Marie-Ampere.(5.4.2019).
Sharma Neetesh, Tabandeh Armin & Gardoni Paolo. (2018). Resilience analysis: a mathematical formulation to model resilience of engineering systems. Sustainable and Resilient Infrastructure 3(2): 49-67.
Smuts Jan. (1926). Holism and evolution. New York: Macmillan Company.
Southwick Steven & Charney Dennis. (2018). Resilience: The science of mastering life's greatest challenges. Cambridge: Cambridge University Press.
Stevens-Rumann Camille, Kemp Kerry, Higuera Philip, Harvey Brian, Rother Monica, Donato Daniel, Morgan Penelope & Veblen Thomas. (2018). Evidence for declining forest resilience to wildfires under climate change. Ecology Letters 21(2): 243-252.
Suarez-Tangil Guillermo, Palomar Esther, Ribagorda Arturo & Sanz Ivan. (2015). Providing SIEM systems with self-adaptation. Information Fusion 21: 145-158. Haettu osoitteesta: http://www.sciencedirect.com.libproxy.tuni.fi/science/article/pii/S1566253513000535.
Taskinen Santeri. (2018). Eettinen hakkerointi systeemiteoreettisessa tarkastelussa. Tampereen yliopisto, Tampere.
The World Bank. (2019). GDP (current US$). Haettu osoitteesta: https://data.worldbank.org/indicator/ny.gdp.mktp.cd.(28.5.2019).
Tierney Kathleen. (2014). The social roots of risk: Producing disasters, promoting resilience. USA: Stanford Business Books, an imprint of Stanford University Press.
Tieteen termipankki. (2019a). Anturi. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Ymp%C3%A4rist%C3%B6tieteet:anturi.(12.6.2019).

Tieteen termipankki. (2019b). Biologia: Kompleksi. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Biologia:kompleksi.(24.5.2019).
Tieteen termipankki. (2019c). Biologia: Synergia. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Biologia:synergia.(29.6.2019).
Tieteen termipankki. (2019d). Filosofia: Analyysi. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:analyysi.(28.6.2019).
Tieteen termipankki. (2019e). Filosofia: Dualismi. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:dualismi.(24.5.2019).
Tieteen termipankki. (2019f). Filosofia: Emergentti materialismi. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:emergentti_materialismi.(24.6.2019).
Tieteen termipankki. (2019g). Filosofia: Hermeneutiikka. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:hermeneutiikka.(13.5.2019).
Tieteen termipankki. (2019h). Filosofia: Idealismi. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:idealismi.(24.5.2019).
Tieteen termipankki. (2019i). Filosofia: Induktio. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:induktio.(13.5.2019).
Tieteen termipankki. (2019j). Filosofia: Käsite. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:k%C3%A4site.(13.5.2019).
Tieteen termipankki. (2019k). Filosofia: Monismi. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:monismi.(24.5.2019).
Tieteen termipankki. (2019l). Filosofia: Emergenssi. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:emergenssi.(21.4.2019).
Tieteen termipankki. (2019m). Filosofia: Ilmiö. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:ilmi%C3%B6.(12.5.2019).
Tieteen termipankki. (2019n). Filosofia: Tieteenfilosofia. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:tieteenfilosofia.(12.5.2019).
Tieteen termipankki. (2019o). Hermeneuttinen kehä. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Filosofia:hermeneuttinen_keh%C3%A4.(12.6.2019).
Tieteen termipankki. (2019p). Nimitys: Antagonismi. Haettu osoitteesta: http://tieteentermipankki.fi/wiki/Nimitys%3Aantagonismi.(26.6.2019).
Tieteen termipankki. (2019q). Ympäristötieteet: Entropia. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Ymp%C3%A4rist%C3%B6tieteet:entropia.(22.4.2019).
Tieteen termipankki. (2019r). Filosofia: Kontingenssi. Haettu osoitteesta: https://tieteentermipankki.fi/wiki/Filosofia:kontingenssi.(11.4.2019).
Tietotekniikan termitalkoot. (2007). Palomuuri. Haettu osoitteesta: http://www.tsk.fi/tsk/termitalkoot/haku-266.html?page=get_id&id=ID0058&vocabulary_code=TSKTT.(26.6.2019).
Tokody Dá. (2018). Digitising the European industry - holonic systems approach. Procedia Manufacturing 22: 1015-1022.
Toyota Masatsugu, Spencer Dirk, Sawai-Toyota Satoe, Jiaqi Wang, Zhang Tong, Koo Abraham, Howe Gregg & Gilroy Simon. (2018). Glutamate triggers long-distance, calcium-based plant defense signaling. Science 361(6407): 1112-1115.
Traficom. (2018). Kyberturvallisuuskeskuksen esittelymateriaali. Cyber Security Nordic -messut, Helsingin messukeskus: Traficom, Kyberturvallisuuskeskus.
TrustRadius. (2019). Unified endpoint management (UEM) overview. Haettu osoitteesta: https://www.trustradius.com/unified-endpoint-management-uem.(26.5.2019).
Tuomaala Jirko. (2018). Seuraavan sukupolven palomuurin valinta. Lahden ammattikorkeakoulu, Lahti.
Tusaie Kathleen & Dyer Janyce. (2004). Resilience: A Historical Review of the Construct. Holistic Nursing Practice 18(1): 3-10.
Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. (2016). VAHTI 2/2016 toiminnan jatkuvuuden hallinta. Helsinki: Valtiovarainministeriö.
Van der Kleij, Kleinhuis Geert & Young Heather. (2017). Computer security incident response team effectiveness: A needs assessment. Frontiers in Psychology 8: 2179.
Vataja Katri. (2019). Monimutkainen, systeeminen vaikuttavuus. Haettu osoitteesta: https://www.sitra.fi/blogit/monimutkainen-systeeminen-vaikuttavuus/.(16.4.2019).

Virta Sirpa. (2012). Turvallisuuden tutkimus. Tieteenalat ja monitieteisyyden lähtökohtia. Tiede ja ase 69: 112-126.
von Bertalanffy Ludwig. (1968). General system theory. New York: George Braziller Inc.
von Neumann John. (1945). The first draft of a report on the EDVAC. Moore School of Electric Engineering University of Pennsylvania. Haettu osoitteesta: https://archive.org/stream/first-draftofrepo00vonn#page/n1/mode/2up.
von Solms Rossouw & van Niekerk Johan. (2013). From information security to cyber security. Computers & Security 38: 97-102. Haettu osoitteesta: http://www.sciencedirect.com.lib-proxy.tuni.fi/science/article/pii/S0167404813000801.
Wang Hua, Han Donghai & Jiang Jingchun Jason. (2018). Nicira Inc., assignee. Port Mirroring in Overlay Networks. Patent 15/421365.
Wiener Norbert. (1948). Cybernetics. New York: Wiley.
Winters Timothy. (2019). Next Generation Firewall Testing Using Open Standards. Security 56(6): 40.
Woods David. (2015). Four concepts for resilience and the implications for the future of resilience engineering. Reliability Engineering and System Safety 141: 5-9.
Working Party of the Royal College, of Physicians. (2003). The vegetative state: guidance on diagnosis and management. Clinical Medicine, Journal of the Royal College of Physicians 3(3): 249-254.
Zimmerman Carson. (2014). Ten strategies of a world-class cybersecurity operations center. USA: MITRE Corporate Communications and Public Affairs.
Åhman Helena & Gustafsberg Harri. (2017). Tilannetaju: Päätä paremmin. Helsinki: Alma Talent Pro.
Åhman Helena & Rauhala Ilona. (2017). Tilannetietoisuus. Haettu osoitteesta: https://www.youtube.com/watch?v=k6gR23rA9TU.(12.6.2019).

LIITTEET

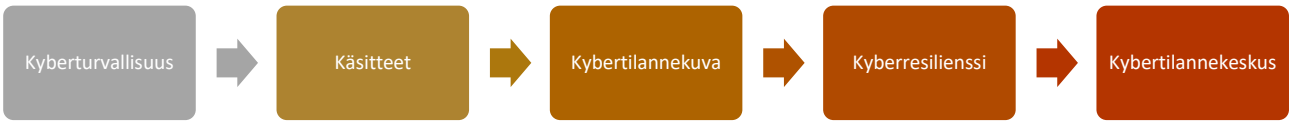
Liite 1. Kvalitatiivinen puolistrukturoitu haastattelurunko asiantuntijoille

Hei! Olen Santeri Taskinen Tampereen yliopiston Johtamiskorkeakoulusta ja tutkin kybertilannekeskusten vaikutusta organisaatioiden kyberresilienssiin. Haastattelen kyberturvallisuuden asiantuntijoita osana tutkimustani. Olisiko teillä aikaa vastata kysymyksiin liittyen kybertilannekuvaan, tilannekuvatiedon tarpeellisuuteen ja vaikutuksiin organisaatioiden kyberresilienssiin? Aikaa haastatteluun kuluisi noin 30 minuuttia.

Alustavat kysymykset (noin 1-5 minuuttia):

1. Voinko tallentaa keskustelumme litterointia varten? (Kyllä/Ei)
    - Analysoin tallennetun aineiston osaksi tutkimusraporttini tuloksia.
2. Kertoisitteko oman nimenne?
    - Käsittelen haastateltuja tutkimusraportissani nimettömänä koodattuna.
3. Kertoisitteko organisaation ja työtehtävän, jossa olette töissä?
    - Saanko mainita tutkimusraportissani organisaation/toimialan/työtehtävän, jossa olette töissä ilman nimeänne? (Organisaatio / Toimiala / Työtehtävä)
4. Montako vuotta olette olleet töissä kyberturvallisuusalalla?
    - Onko teillä kokemusta kybertilannekuvatoiminnasta tai kyberresilienssiin liittyvistä asioista?
    - Ovatko kybertilannekeskukset teille tuttuja?
        - Millaisista yhteyksistä ne ovat teille tuttuja?
        - Miksi ajattelette, että ne eivät ole tuttuja?
    - Saanko mainita tutkimusraportissani, montako vuotta olette olleet alalla töissä ja mainita siitä, kuinka tuttuja kybertilannekeskukset ovat teille? (Kyllä/Ei)

Varsinaiset kysymykset (noin 20-29 minuuttia) teemoittain:



Kyberturvallisuus

Lyhyesti: Mitä kyberturvallisuus mielestänne tarkoittaa?

Kyberturvallisuus (engl. cyber security) tarkoittaa kaikkien toimijoiden ja toimintojen kyberkokonaisuudesta aiheutuvaa turvallisuuden tilannetta. Kyberturvallisuuteen kuuluvat tietoturvallisuuden ja kyberfyysisten systeemien turvallisuuden kaikki osa-alueet. Tietotur-

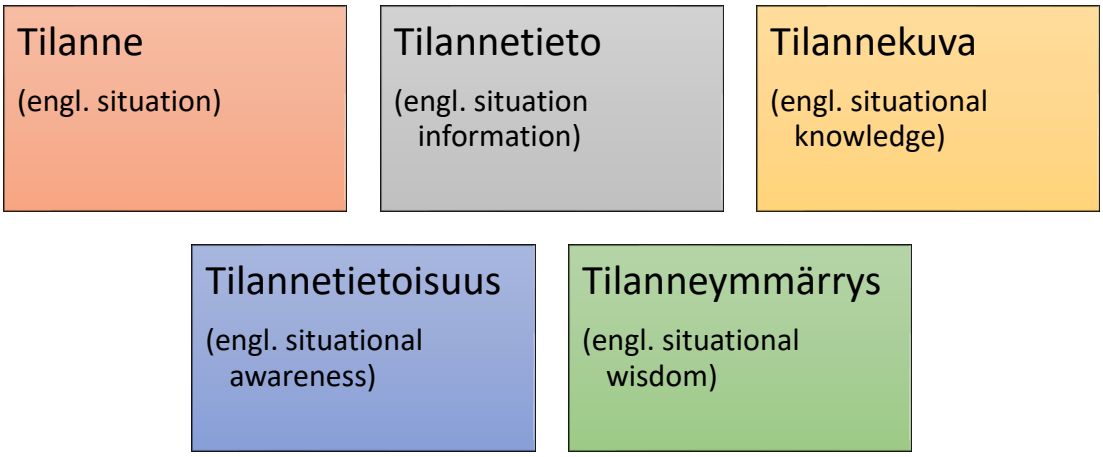
van osa-alueita ovat fyysinen tietoturva, hallinnollinen tietoturva, tietoaineisto-, tietoliikenne- ja ohjelmistoturvallisuus sekä yksityisyyden suojan asiat. Kyberturvallisuuteen kuuluvat lisäksi kriittisten järjestelmien turvallisuus, kybersota, tiedustelutoiminta sekä kyberterrorismi. Myös fyysisen maailman ohjaaminen tietoverkkoja tai -tekniikkaa hyväksi käyttäen kuuluu kyberturvallisuuden käsitteen piiriin. (Taskinen 2015, Harju 2015)

Miltä määritelmä kuulostaa?

Käsitteet

Käydään läpi muutamia käsitteitä. Esitän seuraavaksi viisi käsitettä lapuilla. **Pohtikaa, mitä käsitteet mielestänne tarkoittavat ja mikä yhteys niillä on toisiinsa?** Tässä ei ole oikeaa eikä väärää vastausta.

1. Tilanne (engl. situation)
2. Tilannetieto (engl. situation information)
3. Tilannekuva (engl. situational knowledge)
4. Tilannetietoisuus (engl. situational awareness)
5. Tilanneymmärrys (engl. situational wisdom)



Kerrataan vielä edellisen teeman määritelmä: Tutkimuksessani kyberturvallisuus on toimijoiden ja toimintojen kyberkokonaisuudesta aiheutuva turvallisuuden **tilanne**.

1. Tilanne: on asioiden tilan ja olosuhteiden olemus tietyssä ajassa ja paikassa.
2. Tilannetieto: on yksi tosi ja perusteltu asian tila ja olosuhde tietyssä ajassa ja paikassa.
3. Tilannekuva: Tilannetiedoista jokaisen ihmisen itse muodostama kuva tai käsitys tilanteesta.
4. Tilannetietoisuus: Toimijan tilannekuvan ja resurssien tuntemisen muodostama tulkinta tilanteessa toimimisesta.
5. Tilanneymmärrys: Kyky ennustaa ja ennakoida laajasti tekijöitä, jotka vaikuttavat tilanteen kehittymiseen.

Mitä ajattelet edellisistä määritelmistä?

Kybertilannekuva

1. Organisaationäkökulmasta: Kenellä on vastuu kybertilannetietojen keräämisestä? Entä jakamisesta muille?
2. Mihin yhteistä ja jaettua kybertilannekuvaa tarvitaan?
3. Mitä tapahtuisi, jos kybertilannetietoa ei ole tai se on suppeaa? Entä jos sitä on valtavasti tai se on ristiriitaista?

Näytä elintärkeiden toimintojen listaa.

Yhteiskunnan elintärkeät toiminnot. (Turvallisuuskomitea, 2018)

Viimeisimmän julkaistun yhteiskunnan turvallisuusstrategian mukaan "***johtaminen*** *on yksi* ***seitsemästä*** *elintärkeästä toiminnosta, jotka ovat yhteiskunnalle kaikissa tilanteissa* ***ylläpidettäviä*** *ja* ***välttämättömiä*** *toimintokokonaisuuksia. Johtaminen* ***luo pohjan*** *muille toiminnoille ja toimintojen turvaamiselle. Johtamiseen liittyvä* ***johtamiskyky*** *halutaan turvata kaikissa* ***tilanteissa*** *ja kaikilla* ***toimintatasoilla****. Turvallisuusstrategian mukaan* ***hyvä johtaminen*** *edellyttää* ***tilannekuvan muodostamista*** *sekä* ***tilanneymmärrystä*** *eli arviota tilanteen tulevasta kehittymisestä. Lisäksi tehokas* ***häiriötilanteiden hallinta*** *edellyttäisi tiivistä* ***yhteistyötä johtamisen****,* ***tilannekuvan*** *ja* ***viestinnän*** *välillä.*" (Turvallisuuskomitea, 2017)

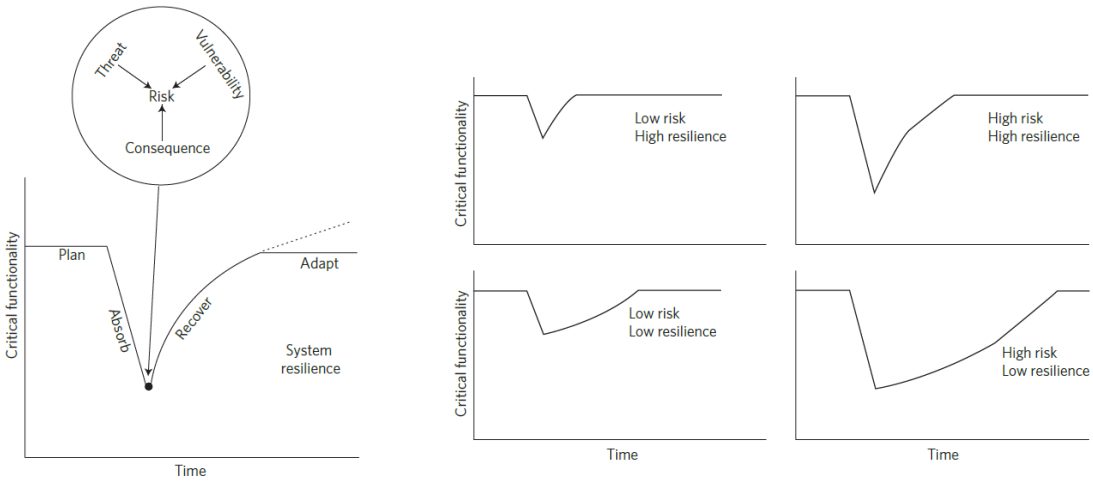
4. Onko pelkkä yhteinen ja jaettu kybertilannekuva riittävä ongelmien ratkaisemiseksi, vai tarvitaanko myös tilannetietoisuutta (tilannekuva + omat resurssit) ja tilanneymmärrystä (ennakointi tilanteen kehittymisestä)? Miksi?

Kyberresilienssi

1. Mitä kyberresilienssi mielestänne tarkoittaa organisaation näkökulmasta?

Näytä resilienssidiagrammia.

Tässä tutkimuksessa kyberresilienssillä tarkoitetaan toimijan – esimerkiksi organisaation, yksikön tai osaston – **kykyä** suunnitella, valmistautua vastaamaan ja toteuttaa haluttua toimintaa keskeytyksettä haitallisista kybertapahtumista huolimatta. **Keskeytyksettömyys** tarkoittaa kykyä kaikissa tilanteissa toipua ja palauttaa toiminta siedettävälle tai normaalia paremmalle tasolle. Normaalien toimintojen häiriö kriisitilanteessa ei saisi näkyä toimijan ulkopuolelle kyvyssä tuottaa haluttua lopputulosta. Mikäli kriisitilanne näkyy toimijan tuottaman toiminnon lopputuloksessa, ei toiminta ole **keskeytyksetöntä**. Keskeytyksettömyyteen vaaditaan kyky palauttaa, muuttaa tai muokata normaaleja toimintoja kriisitilanteessa, jotta toimintojen jatkuvuus voidaan varmistaa. (Björck ym. 2015, 312)



Resilienssin hallinnan viitekehys sisältää **riskien hallinnan**: Riskin vaikutus organisaatioon määritellään **uhasta**, **haavoittuvuudesta** ja **seurauksista**, joka muodostaa haitallisen tapahtuman (esim. hajautettu palvelunestohyökkäys). Tämä tapahtuma näkyy elintärkeiden toimintojen menetyksenä ajan kuluessa. Toiminnallisesti resilienssi kuvataan tietyn suuruisen riskin toteutumisen yhteydessä elintärkeiden toimintojen **menetyksenä**, **palautumisena** tai **kehittymisenä**. Vaiheita ovat 1. **valmistautuminen** 2. **mukautuminen** 3. **toipuminen** 4. **sopeutuminen**. Käyrän kaltevuus mukautumis- ja toipumisvaiheessa osoittaa resilienssin **tason** riskin toteutuessa järjestelmässä. Erittäin resilientti eli muuntokykyinen organisaatio tai järjestelmä **kykenee** muuttamaan toimintatapojaan siten, että jopa alkuperäinen resilienssitaso **ylittyy** eli tapahtuu **kehitystä**. (Linkov, et all., 2014)

2. Mitä ajattelet tästä kyberresilienssin määritelmästä? Toimiiko edellä esittämäni malli kyberturvallisuusasioissa?
3. Miten riskienhallinta ja kyberresilienssi liittyvät toisiinsa?
4. Miten organisaation kyberresilienssiin voidaan vaikuttaa?

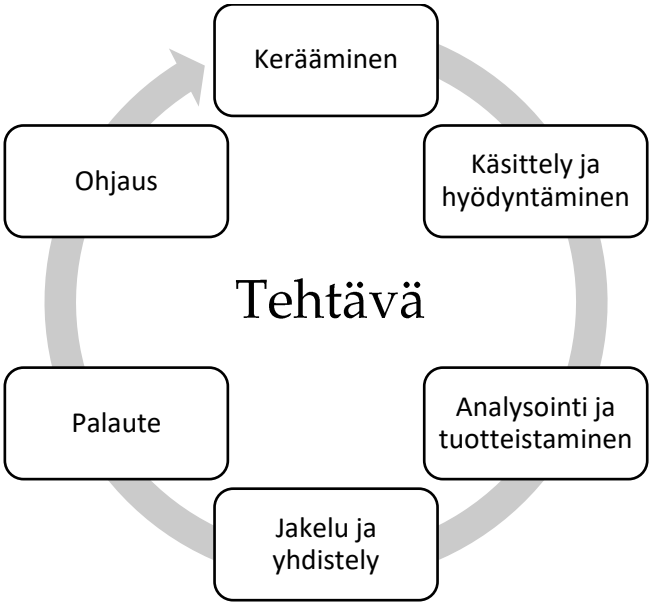
Kybertilannekeskus

1. Mikä on kybertilannekeskuksen tehtävä (engl. CSOC, Cyber Security Operations Center)?
2. Mitä tuotetaan, Miten se toimii päivittäin, Milloin (24/7)? ja Missä?
3. Mitä seikkoja kybertilannekeskuksen perustamiseen ja ylläpitoon liittyy?
4. Millaisissa rooleissa olevia ihmisiä kybertilannekeskuksessa työskentelee? Miksi?
5. Miten kybertilanneTIETO kerätään käytännössä?
6. Mitä kybertilanneTIETOa tarvitaan kybertilanneKUVAn muodostamiseen?
7. Miten kybertilanneKUVA luodaan ja ylläpidetään käytännössä?
8. Miten kybertilanneTIETOISUUS muodostuu kybertilannekeskuksessa?
9. Miten kybertilanneYMMÄRRYS selkeytyy?
10. Mitä hyötyä kybertilannekeskuksista on organisaatioille? Mitä haittaa organisaatioille?
11. Organisaatio voi:
    1. olla ilman kybertilannekeskusta,
    2. perustaa kybertilannekeskuksen itse tai
    3. ostaa sen palveluna.

Millä ehdoilla toimintamalli tulisi valita vai onko jotakin muita toimintamalleja olemassa?

Yhteiskunnan turvallisuusstrategiassa todetaan, että ”monimuotoisten ja nopeasti kehittyvien **häiriötilanteiden hallinta** edellyttää **oikea-aikaista** ja **joustavaa** reagointia. Lisäksi edellytetään, että toiminnan **koordinointi** ja **tiedonkulku** varmistetaan eri viranomaisten ja muiden **turvallisuustoimijoiden yhteistoiminnalla**.” (Turvallisuuskomitea, 2017)

12. Miten ajattelet tästä? Kuinka yhteistoiminta arviosi mukaan toteutuu nykyään kybertilannekeskusten välillä? Viranomaiset? Miten yhteistoimintaa voisi kehittää?
13. Tunnistatko jotakin erityisiä haasteita tai tilanteita, jolloin organisaatio ei voisi tai halua hyödyntää kybertilannekeskuksia toiminnassaan?
14. Millaisia tällaiset organisaatiot ovat?
15. Käytetäänkö kybertilannekeskuspalveluita tarpeeksi? Miksi/ Miksi ei? Miten se ilmenee käytännössä?
16. Vaikuttaako (vaikuttavuus) kybertilannekeskus oikeasti organisaatioihin ja niiden toimintaan, kuten kyberresilienssiin?
17. Miten kybertilannekeskuksella vaikutetaan organisaation kyberresilienssiin?
18. Mihin kyberresilienssin osa-alueisiin (näytä resilienssikaaviota) vaikutetaan? Entä kyberturvallisuuden todelliseen tasoon?
19. Mihin kyberresilienssiin liittyviin asioihin kybertilannekeskuksella ei voida vaikuttaa? Miksi?



Tiedusteluympyrä. (CIA, 2018)

Lopuksi pohditaan, mikä on **kybertilannekeskuksen** ja **tiedustelun** suhde toisiinsa. Yleisesti tiedetään, että **tiedustelu tuottaa tietoa päätöksenteon tueksi**. Tiedustelun vaiheita ovat: tiedon kerääminen, käsittely, analysointi, jakaminen, palauteen vastaanottaminen ja ohjaus. (Näytä tiedusteluympyrää)

20. Liittyykö kybertilannekeskustoiminta mitenkään tiedusteluun?

21. Miten / Miksi ei? Yksityisyyden suojan huomioiminen?

Haastattelun aiheena oli kybertilannekeskusten vaikutus organisaatioiden kyberresilienssiin. Onko jotakin olennaista jäänyt kysymättä tai haluaisitteko lisätä tähän loppuun vielä jotakin?

Kiitos paljon ajastanne!

Liite 2. Graafinen käsitekartta kyber- ja tietoturvallisuuden eroista